Національний університет водного господарства та природокористування
Навчально-науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного врядування

Пояснювальна записка
до дипломної роботи

бакалавр
(освітньо-кваліфікаційний рівень)
на тему:

ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ТА ЗАБЕЗПЕЧЕННЯ ЗБЕРЕЖЕНОСТІ ЕЛЕКТРОННИХ АРХІВНИХ РЕСУРСІВ (НА ПРИКЛАДІ ДЕРЖАВНОГО АРХІВУ РІВНЕНСЬКОЇ ОБЛАСТІ)

Виконав: студент 4 курсу, групи ІБАС-41
спеціальності 029 «Інформаційна,
бібліотечна та архівна справа»

Шамало Ілля Максимович

Керівник: к.і.н., доцент кафедри менеджменту
та публічного врядування
Цецик Ярослав Петрович

Рівне-2026

Форма № Н-9.01

Національний університет водного господарства
та природокористування
(повне найменування вищого навчального закладу)

Навчально-науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного врядування
Рівень вищої освіти бакалавр
Спеціальність 029 «Інформаційна, бібліотечна та архівна справа»
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувачка кафедри
менеджменту та публічного
врядування
_____ Л.Х. Тихончук
“__”_____ 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ШАМАЛО ІЛЛІ МАКСИМОВИЧУ
(прізвище, ім’я, по батькові)

1. **Тема роботи:** Проєктування системи захисту та забезпечення збереженості електронних архівних ресурсів на прикладі Державного архіву Рівненської області

Керівник роботи: к.і.н., доцент кафедри менеджменту та публічного врядування Цецик Ярослав Петрович
затверджені наказом вищого навчального закладу від “ 27.04.2026”
2026 р. С №503

2. Строк подання студентом роботи « 16 » червня» 2026 р.

3. Вихідні дані до роботи: нормативно-правові акти, статистичні дані, підручники, посібники, монографії, періодичні видання.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Теоретичні основи та еволюція концепцій довгострокового цифрового збереження 2. Аналіз системи цифрового архівування у державному архіві Рівненської області 3. Архітектурні зміни та проєктування системи довгострокового збереження цифрових об'єктів у державному архіві рівненської області

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень): 1. Схема роботи RAID 1. 2. Схема роботи RAID 5.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Цецик Я. П., доцент	01.05.2026	10.05.2026
Розділ 2	Цецик Я. П., доцент	11.05.2026	25.05.2026
Розділ 3	Цецик Я. П., доцент	26.05.2026	05.06.2026

7. Дата видачі завдання « » 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів	Примітка
1.	Вступ Розділ 1. Теоретичний розділ	до 10.05.2026	
2.	Розділ 2. Аналітичний розділ	до 25.05.2026	
3.	Розділ 3. Проектування, обґрунтування, оптимальні рішення, їх впровадження	до 05.06.2026	
4.	Перевірка випускної кваліфікаційної роботи на наявність текстових збігів, оформлення презентації, документів та підготовка до захисту	до 16.06.2026	

Студент

_____ Ілля ШАМАЛО
(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи

_____ Ярослав ЦЕЦИК
(підпис) (прізвище та ініціали)

ЗАЯВА
щодо самостійності виконання випускної кваліфікаційної роботи

Я, Шамало Ілля Максимович, студент 4 курсу групи ІБАС-41 ННІЕМ

ЗАЯВЛЯЮ:

моя випускна кваліфікаційна робота на тему «Проєктування системи захисту та забезпечення збереженості електронних архівних ресурсів на прикладі Державного архіву Рівненської області», яка надається в екзаменаційну комісію із захисту кваліфікаційних робіт зі спеціальності 029 «Інформаційна, бібліотечна та архівна справа» для захисту, виконана самостійно і не містить плагіату.

Всі запозичення з друкованих та електронних джерел, у тому числі із захищених раніше випускових кваліфікаційних робіт мають відповідні посилання.

Я не використовував(ла) шахрайські методи маніпуляції з текстом (заміна букв, інтервали, мікропробіли, білі знаки, парафрази та ін.).

Інструменти штучного інтелекту використовував(ла) без порушення академічної доброчесності.

Я ознайомлений(а) з чинним Порядком перевірки навчальних, кваліфікаційних, навчально-методичних та наукових робіт на наявність ознак академічного плагіату в НУВГП та Положенням про академічну доброчесність в НУВГП, за яким виявлення плагіату є підставою для відмови в допуску моєї роботи до захисту та застосування відповідних санкцій (академічної відповідальності).

Дата *Підпис*

АКТ
перевірки випускної кваліфікаційної роботи
автора *Шамало Іллі Максимовича*
на рівень запозичень та можливих маніпуляцій з текстом

Відповідно до даних системи StrikePlagiarism файл «ДИПЛОМ_ШАМАЛО_2.docx»

містить: 4.63% коефіцієнта подібності; 1.71% коефіцієнта цитованості;
0 замінених букв; 0 інтервалів; 0 мікропробілів; 0 білих знаків;
25 парафраз.

За результатами перевірки засвідчую, що:
автор кваліфікаційної роботи ***Шамало Ілля Максимович***:

- самостійно виконав кваліфікаційну роботу;
- коректно посилався на використані інформаційні джерела;
- в роботі відсутні ознаки академічної недоброчесності.

Керівник кваліфікаційної роботи Ярослав ЦЕЦИК

Дата

StrikePlagiarism.com

Національний університет водного господарства та природокористування

Документ прийнятий

Метадані

ДОКУМЕНТ

Заголовок
ДИПЛОМ_ШАМАЛО_2.docx

Автор	Науковий керівник / Експерт	ІД документу
Шамало Ілля Максимович	**Шамало Ілля Максимович**	**334344379**

ОРГАНІЗАЦІЯ

Назва організації	підрозділ
National University of Water and Environmental Engineering	**National University of Water and Environmental Engineering**

ЗВІТ

Дата звіту	Дата редагування
6/16/2026	**---**

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

13181
Кількість слів

КЦ

109832
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	0
Інтервали	A	0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)	a	25

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

ЗМІСТ

ВСТУП

Актуальність теми. Швидке збільшення кількості цифрових документів та їх активне використання в установах управління інформацією суттєво змінило підходи до управління інформацією. Ця зміна діловодства та збереження спадщини продемонструвала швидкість і легкість короткострокового транскордонного поширення даних. Проте водночас виявила значну нестачу підходів до забезпечення довгострокової життєздатності цифрової інформації. Інформаційне суспільство стикається з ризиком безповоротної втрати інформації через деградацію фізичних носіїв, відсутність стандартизованих форматів та надзвичайно швидкого технологічного застарівання апаратно-програмних комплексів [42], [64], [31], [15], [13], [3].

Основна проблема проблема полягає в нестійкій природі цифрової інформації, яка кардинально відрізняється від традиційних фізичних носіїв, таких як пергамент, папір або кіноплівка. Цифрові об'єкти не є статичними фізичними одиницями. Вони являють собою логічні конструкції, що потребують багатошарової програмної та апаратної інтерпретації для коректного відтворення. Вони легко піддаються випадковому пошкодженню на рівні бітових потоків або зловмисній непомітній зміні, що безпосередньо ставить під загрозу їхню юридичну автентичність, історичну цілісність і доказову силу [42], [64], [37], [58].

Невід'ємна залежність складних мультимедійних ресурсів, динамічних баз даних та спеціалізованого програмного забезпечення від пропрієтарних середовищ робить їх недоступними поза межами первинних середовищ [64], [33], [63] .

Ця проблема додатково загострюється через зовнішні чинники, зокрема політичну нестабільність та воєнні дії. В умовах повномасштабного вторгнення в Україну фізичні та цифрові архіви перетворилися на стратегічні мішені, свідоме знищення яких агресором має на меті стирання національної ідентичності, руйнування інституційної пам'яті та дестабілізацію державного управління [18], [15], [3], [19].

Ефективний захист цифрових архівів потребує інтеграції міжнародних стандартів збереження, сучасних апаратних рішень та актуальної нормативної бази щодо управління кіберризиками. [37], [58], [38], [39], [40].

Метою дипломної роботи є дослідження теоретичних та методологічних основ довгострокового цифрового збереження та розроблення рекомендацій щодо удосконалення системи електронного архівування на прикладі **Державного архіву Рівненської області**.

1. дослідити теоретичні основи та еволюцію концепцій довгострокового збереження цифрової інформації;
2. проаналізувати міжнародні моделі цифрового архівування та технологічні стратегії подолання апаратно-програмного застарівання;
3. проаналізувати нормативно-правову базу та специфіку цифровізації архівів в умовах воєнного стану в Україні;
4. охарактеризувати діяльність та сучасний стан інфраструктури в Державному архіві Рівненської області;
5. оцінити організацію процесів цифрового збереження, управління метаданими та кібербезпеки у Державному архіві Рівненської області;
6. дослідити проблематику функціонування та виявити ключові вразливості електронних ресурсів досліджуваної установи;
7. навести напрями покращення ефективності системи збереження цифрових об'єктів;

8. розробити практичні рекомендації щодо впровадження сучасних технологій, безпекових стандартів та міжнародних моделей у Державному архіві Рівненської області;

Об’єкт дослідження - процес довгострокового збереження, управління та захисту життєвого циклу цифрових об'єктів у сучасних архівних системах.

Предмет дослідження - організаційні, технологічні, нормативні та безпекові механізми функціонування цифрових архівів на міжнародному рівні та у вітчизняному державному секторі.

До **методів дослідження**, що були використані у роботі, можна віднести:

1. бібліографічний та термінологічний методи, які використано для глибокого аналізу фахової наукової літератури, міжнародних стандартів (ISO, CCSDS) та нормативно-правових актів;
2. системно-структурний аналіз, який застосовано для декомпозиції еталонних архітектур (зокрема OAIS та PREMIS) на базові функціональні компоненти;
3. порівняльно-аналітичний метод, що дозволив зіставити ефективність різних технологічних стратегій (міграції, емуляції, інкапсуляції) та інструментів оцінки зрілості (ISO 16363 та DPC RAM);
4. табличний метод, який використано для логічної систематизації кількісних і якісних показників, метрик кібербезпеки та вітчизняної статистики цифровізації [37], [58], [38], [27], [8], [39] .

Інформаційною базою дослідження є міжнародні нормативні документи серій ISO та Consultative Committee for Space Data Systems (CCSDS), аналітичні звіти провідних світових інституцій, зокрема Національного управління архівів та документації США (NARA) та Коаліції цифрового збереження (DPC), публікації у фахових наукових виданнях, а

також чинні закони України, національні стандарти (ДСТУ) та офіційні аналітичні дані Міністерства юстиції і Державної архівної служби України щодо реалізації програм електронного урядування.

Основні наукові положення та практичні результати кваліфікаційної роботи були представлені у вигляді тез у збірник конференції: XV Міжнародна науково-практична конференція «Актуальні проблеми теорії і практики менеджменту та публічного врядування в контексті євроінтеграції», 21 травня 2026 рік.: на тему: «Міжнародні еталонні моделі цифрового архівування та екосистема збереження метаданих», а також було опубліковано наукову статтю у студентському науковому журналі «Вісник науки та освіти» № 4(46) 2026 на тему: «Роль цифрових технологій у зберіганні архівної інформації» [17].

Структура й обсяг роботи. Наукова робота складається зі вступу, трьох основних розділів (поділених на відповідні підрозділи), висновків і списку використаних джерел. Логіка викладу підпорядкована послідовному переходу від фундаментальних теоретичних моделей збереження до інженерно-технічних рішень та їх практичної імплементації.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА ЕВОЛЮЦІЯ КОНЦЕПЦІЙ ДОВГОСТРОКОВОГО ЦИФРОВОГО ЗБЕРЕЖЕННЯ

1.1. Проблематика «цифрових темних віків» та еталонні моделі та система збереження метаданих

Масове впровадження електронного документообігу докорінно змінює класичні підходи до архівування. Замість зосередження виключно на захисті фізичного носія, на перший план виходить управління цифровими даними та підтримка їхніх форматів. Раніше функція архіву чи бібліотеки полягала у створенні фізичного середовища, де матеріальні носії - папір, пергамент, фотоплівка чи мікрофіші - могли б зберігатися століттями завдяки стабілізації температури, вологості та мінімізації впливу ультрафіолетового випромінювання. Проте цифрова природа сучасних інформаційних об'єктів робить такі виключно пасивні, фізичні підходи вкрай недостатніми та застарілими. Електронний запис не є єдиним, цілісним матеріальним об'єктом. Це надзвичайно складна конструкція, що складається з потоків бітів, які потребують безперервної інтерпретації через багатошарову, крихку архітектуру фізичного апаратного забезпечення, драйверів, операційних систем і прикладних програм. Без синхронної взаємодії всіх елементів цього середовища цифрові дані миттєво перетворюються на випадковий набір символів, втрачаючи свою цінність [42], [64] .

Порушення взаємодії між апаратним та програмним забезпеченням робить цифрові дані нечитабельними. Легкість масового створення електронних документів різко контрастує зі складністю їхнього тривалого технічного супроводу, що формує реальну загрозу втрати інформаційних масивів. [42], [64].

Термін «цифрові темні віки» (Digital Dark Ages), який вперше запровадив дослідник Куні Террі під час конференції IFLA у 1997 році, ідеально відображає цей гіпотетичний, але математично та технологічно обґрунтований сценарій. Сутність проблеми, за визначенням Куні Т., полягає в тому, що старіння форматів, програмного забезпечення та апаратних засобів зробить сучасну інформацію нечитабельною, якщо суспільство не буде постійно, проактивно її підтримувати. Якщо людство не матиме змоги прочитати застарілі файлові формати, або якщо апаратне забезпечення для зчитування старих носіїв (магнітних стрічок, дискет, специфічних оптичних дисків) перестане існувати, сучасна епоха залишить по собі менше читабельних історичних записів, ніж епоха античності. Ця втрата зумовлюється не лише фізичною деградацією носіїв інформації - явищем, відомим в інженерії як «гниття бітів» (bit rot) або втрата магнітної коерцитивності, - а передусім логічною нездатністю майбутніх комп'ютерних систем розпізнати й розшифрувати формати файлів [42].

Фундаментальний економічний та технологічний конфлікт полягає в тому, що постійна комерційна необхідність IT-корпорацій оновлювати програмне забезпечення та виводити на ринок нові продукти призводить до штучного скорочення життєвого циклу підтримуваних форматів. Як влучно зазначив дослідник Ротенберг Джефф ще у 1999 році, архіви та бібліотеки опинилися в «технологічному сипучому піску» (technological quicksand). Інформаційні інституції змушені безперервно витрачати обмежені бюджети на перенесення петабайтів даних на нові платформи лише для того, щоб підтримувати їх базову доступність. Щойно завершується один цикл міграції, технологічний прогрес робить нову платформу застарілою, змушуючи починати процес заново [64].

Відповідно, виникла потреба у створенні моделей, які б дозволили інституціям оцінити реальну вартість тривалого зберігання файлів. Міжнародні проєкти LIFE (Lifecycle Information for E-Literature) та KRDS (Keeping Research Data Safe) вперше адаптували індустріальний підхід розрахунку вартості життєвого циклу спеціально для цифрових архівів. Наприклад, дослідження KRDS довело: безпосереднє довгострокове зберігання бітів на серверах становить лише близько 15% від загальних витрат установи, тоді як левову частку ресурсів (до 55%) поглинають процеси початкового збору, приймання (Ingest) та ручної валідації даних архівістами. За математичною моделлю LIFE, вартість підтримки електронного об'єкта лише зростає з плином років через необхідність боротьби із застаріванням, що остаточно доводить економічну нежиттєздатність пасивних стратегій збереження («збережи і забудь») [26].

Масштаб цієї інституційної кризи яскраво ілюструють сучасні дослідження, проведені у сфері наукового книговидання - секторі, який традиційно вважається еталоном відповідальності за збереження знань. Масштабний аналіз, здійснений дослідницькою групою на чолі з Івом Мартіном, що охопив понад 7,4 мільйона цифрових ідентифікаторів об'єктів (DOI), продемонстрував катастрофічний розрив між фактом публікації та фактом довгострокового збереження [31].

У таблиці 1.1 наведено узагальнені результати цього аналізу [31].

Статус збереження об'єктів DOI (вибірка 7 438 037)	**Відсоток від вибірки**	**Кількість наукових робіт**

Присутні принаймні в одному архіві	58,38%	4 342 368
Жодних ознак збереження (Unpreserved)	27,64%	2 056 492
Виключені з вибірки (неповнота метаданих)	13,98%	1 039 177

Табл. 1.1. Статус збереження наукових публікацій за ідентифікаторами DOI [31].

Наведені дані доводять відсутність єдиного та системного підходу до збереження цифрових даних серед установ. Базовий поріг надійності, який вимагає децентралізованого зберігання копій принаймні у трьох незалежних архівах, змогли підтвердити менш ніж 1% організацій (лише 204 члени системи Crossref). Майже третина учасників глобальної системи реєстрації взагалі не бере участі в жодних спеціалізованих програмах збереження. Це емпірично доводить надзвичайно важливу тезу: формальна публікація в мережі Інтернет чи присвоєння постійного ідентифікатора не дорівнює архівному збереженню [31].

Проблема втрати інформації загострюється явищем «цифрового розкладання» (digital decay). За даними дослідження Pew Research Center (2024 рік), 38% вебсторінок, що існували у 2013 році, стали недоступними

через десятиліття, що підтверджує крихкість сучасниз цифрових інфраструктур. [57].

Вирішення кризи «цифрових темних віків» вимагає не просто локальних технологічних оновлень, а впровадження жорстких міжнародних архітектур та регуляторних політик. Без них людство неминуче перейде від керованого та структурованого інформаційного середовища до хаотичного простору втрачених, битих і незрозумілих даних [42], [64], [31].

Усвідомлення великих масштабів загрози втрати цифрових даних стимулювало світову спільноту до розроблення уніфікованих концептуальних рамок, здатних забезпечити системний і стандартизований підхід до архівування. Основою у цій сфері стала еталонна модель відкритої архівної інформаційної системи (Open Archival Information System - OAIS), розроблена Консультативним комітетом із космічних систем передачі даних (CCSDS) у 2002 році і згодом формалізована як міжнародний стандарт ISO 14721:2012. Створена початково для вирішення проблеми довгострокового збереження колосальних масивів супутникової телеметрії, які надсилалися різними космічними місіями у несумісних форматах, ця модель швидко довела свою універсальність. Наразі вона визнана де-факто стандартом архітектури для національних архівів, урядових ЦОДів та академічних бібліотек по всьому світу [37], [23].

Модель OAIS пропонує термінологічну та структурну основу, яка докорінно змінює підхід до діловодства. Архівування розглядається не як пасивне складування файлів, а як динамічний процес взаємодії між виробниками інформації, самим архівом та спільнотою споживачів (Designated Community). Структурно OAIS декомпозується на шість ключових функціональних сутностей: приймання (Ingest), архівне зберігання (Archival Storage), управління даними (Data Management), адміністрування

(Administration), планування збереження (Preservation Planning) та доступ (Access) [37], [23], [34].

Основою моделі виступає концепція інформаційного пакета. Він містить як самі цифрові дані, так і інформацію про їх репрезентацію, що дозволяє коректно розшифровувати файли в майбутньому. Життєвий цикл інформації в середовищі OAIS є суворо регламентованим. Спочатку виробник передає до архіву Інформаційний пакет подання (Submission Information Package - SIP). На критичному етапі приймання (Ingest) архів здійснює жорстку валідацію SIP, перевіряючи його на наявність шкідливого коду, цілісність бітових потоків, повноту метаданих та відповідність заявленим інституційним політикам. Лише після успішної верифікації SIP трансформується в Архівний інформаційний пакет (Archival Information Package - AIP). AIP стає єдиною еталонною одиницею довгострокового зберігання; він глибоко інкапсулюється, шифрується і ніколи не надається кінцевому користувачу безпосередньо. Замість цього, на запит споживача система генерує Інформаційний пакет розповсюдження (Dissemination Information Package - DIP), який є похідною копією, адаптованою до сучасних форматів відображення. Такий архітектурний поділ гарантує, що оригінальні дані залишаються недоторканими і захищеними від випадкових модифікацій або технологічних спотворень під час їх експлуатації [37], [23].

Однак у третій редакції моделі OAIS (CCSDS 650.0-M-3 / ISO 14721:2025), опублікованій наприкінці 2024 року, цей підхід було суттєво змінено. Новий стандарт запровадив гнучкість формування пакетів, що легалізує підхід «збережи зараз, опиши пізніше» (ingest first, describe later), а також додав нову проактивну функцію «Preservation Watch» для безперервного моніторингу технологічного застарівання. [59].

Проте ефективне функціонування моделі OAIS неможливе без розгалуженої, стандартизованої системи метаданих. Якщо для традиційних бібліотечних систем було достатньо описових метаданих (наприклад, форматів MARC або Dublin Core) для забезпечення простого пошуку за назвою чи автором, то для цифрових архівів критичним є використання спеціалізованих метаданих збереження. Метадані збереження виконують роль «цифрової палітурки», яка не дозволяє логічній структурі документа розпастися на окремі байти. Де-факто міжнародним стандартом у цій сфері виступає PREMIS (Preservation Metadata: Implementation Strategies), розроблений під егідою Бібліотеки Конгресу США. Остання версія словника даних PREMIS 3.0 детально фіксує вичерпну технічну інформацію, ланцюжки походження (provenance), відомості про програмно-апаратні платформи та інтелектуальні права [58].

Згідно з даталогічною моделлю PREMIS, модель цифрового об'єкта визначається через чотири сутності: Об'єкти (Objects), Події (Events), Агенти (Agents) та Права (Rights). Об'єкти класифікуються на чотири рівні агрегації: Інтелектуальні сутності (наприклад, концептуальний зміст книги чи звіту), Репрезентації (конкретні форми подання, як-от PDF-версія або XML-версія), Файли (безпосередні системні файли) та Потоки бітів (фізичні байти, з яких складається файл). На фоні оновлень стандарту виділяється впровадження семантичних одиниць, таких як preservationLevelRationale, що фіксують аргументацію щодо присвоєння конкретному об'єкту певного рівня збереження (наприклад, законодавча вимога, пошкоджений файл або комерційний запит) [58].

Основною філософською засадою PREMIS є концепція суворої незмінності (immutability) об'єктів. За цією моделлю, якщо в архіві виконується будь-яка дія щодо збереження, яка логічно змінює об'єкт

(наприклад, міграція текстового документа зі старого формату у сучасний стандарт PDF/A), система не переписує і не оновлює початковий файл. Натомість генерується новий цифровий Об'єкт. Сутність «Подія» (Event) детально фіксує криптографічний та історичний зв'язок між оригіналом і похідною копією, зазначаючи точний час і результат конвертації. Документування ролей через сутність «Агент» (Agent), що може бути як посадовою особою, так і автоматизованим скриптом, формує бездоганний ланцюжок довізного контролю (chain of custody). Такий підхід забезпечує довгострокове збереження історичної та правової автентичності записів. Документування кожної зміни формату захищає файл від втрати доказової сили під час його перенесення на нові платформи. [58].

Для фізичного пакування та безпечної передачі метаданих між системами використовується стандарт METS (Metadata Encoding and Transmission Standard). У березні 2025 року Бібліотека Конгресу США випустила мажорне оновлення - METS Version 2, яке сильно спростило XML-схеми та усунуло залежність від застарілого протоколу XLink, повністю адаптувавши стандарт до сучасних хмарних мікросервісних архітектур [43].

На додаток до структурного пакування, сучасна архівна наука переживає трансформацію у семантичному описі документів. Міжнародна рада архівів (ICA) розробила концептуальну модель стандартів Records in Contexts (RiC), формальним поданням якої стала онтологія RiC-O (актуальна версія 1.1 випущена у травні 2025 року). На відміну від застарілих деревоподібних стандартів опису (наприклад, ISAD(G)), RiC-O базується на технологіях семантичного вебу і дозволяє перетворити архів з набору плоских записів на багатовимірний граф знань. Це дає змогу архівам публікувати свої колекції як пов'язані відкриті дані (Linked Open Data), де складні зв'язки між документами, їхніми творцями та історичними подіями

можуть автоматично аналізуватися за допомогою алгоритмів машинного виведення [36].

1.2. Технологічні стратегії подолання апаратно-програмного застарівання, аудит та сертифікація цифрових сховищ

Швидке оновлення програмного забезпечення вимагає від архівів постійних технологічних втручань. Простого зберігання файлів на жорстких дисках наразі недостатньо; необхідно гарантувати можливість їх логічного відтворення у довгостроковій перспективі. Для цього застосовують чотири основні методи: міграцію, емуляцію, інкапсуляцію або фізичне збереження оригінального апаратного забезпечення. [64], [33], [63], [34].

Сьогодні міграція залишається найпоширенішим підходом для збереження текстових документів та баз даних. Її сутність полягає в цілеспрямованому перенесенні цифрових об'єктів із застарілого формату в сучасний (наприклад, масова трансляція баз даних із застарілих dBase у сучасні SQL-структури, або конвертація документів WordPerfect у відкриті формати XML). Водночас цей процес супроводжується ризиком кумулятивної втрати інформації під час багаторазових конвертацій. Під час багаторазових конвертацій можуть непомітно зникати елементи оригінального форматування, складні макроси, закладена функціональність або автентичний вигляд (look and feel) первинного документа. З кожним циклом міграції документ незворотно змінюється, що для архівів історичного або юридичного профілю є критичним недоліком, оскільки ставить під сумнів доказову силу артефакту [63].

Найбільш актуальним цільовим форматом для міграції текстової та графічної документації наразі є стандарт PDF/A-4 (ISO 19005-4:2020), який базується на специфікації PDF 2.0. Його головною інновацією є здатність

безпечно інкапсулювати будь-які довільні вбудовані файли без порушення довгострокової криптографічної цілісності архівного контейнера [56].

Більш досконалою альтернативною є емуляція (Emulation), активним прихильником якої виступає дослідник Грейнджер Стюарт. Замість зміни самого цифрового об'єкта, стратегія емуляції передбачає збереження файлу в його первісному, побітовому вигляді. Паралельно створюються спеціалізовані програмні алгоритми (емулятори), які імітують архітектуру застарілого апаратного забезпечення та операційних систем на сучасних комп'ютерах. Емулятор ефективно транслює команди сучасної машини таким чином, щоб застаріла програма «вважала», що вона функціонує у своєму рідному середовищі. Цей підхід є незамінним для збереження складних, інтерактивних цифрових пакетів, таких як мультимедійні архіви, цифрові твори мистецтва, спеціалізоване геопросторове ПЗ або відеоігри, де взаємодія користувача з інтерфейсом є ключовою частиною документа [33].

Не зважаючи на те, що розробка емуляторів вимагає високих інженерних компетенцій, дослідники просувають ідею створення Універсальної віртуальної машини (Universal Virtual Machine) - стандартизованого, відкритого середовища виконання, здатного зчитувати інструкції минулих архітектур, що дозволило б уникнути нескінченного циклу переписування самих емуляторів під нові операційні системи [33].

Практичною реалізацією цієї системи стала інфраструктура EaaSI (Emulation-as-a-Service Infrastructure). Станом на 2025–2026 роки EaaSI розгорнуто на масштабованій хмарній архітектурі (зокрема на базі кластерів Kubernetes), що дозволяє архівістам і дослідникам отримувати миттєвий інтерактивний доступ до застарілого програмного забезпечення прямо у веб-браузері, без необхідності локального встановлення жодних емуляторів [65].

Стратегія інкапсуляції передбачає розміщення цифрового об'єкта у стандартизований контейнер разом із технічною документацією та специфікаціями формату. Така обгортка містить інструкції, які дозволять інженерам майбутнього декодувати дані без необхідності доступу до оригінального програмного забезпечення [58].

Найменш масштабованою, але важливою для наукових цілей є стратегія збереження технологій (Technology Preservation), відома як підхід «комп'ютерного музею». Вона передбачає фізичне підтримання в робочому стані застарілого апаратного забезпечення (наприклад, старих мейнфреймів або систем читання магнітних перфокарт). Хоча фізична деградація електронних компонентів робить цей метод непридатним для безстрокового використання, він відіграє критичну роль на етапі калібрування сучасних емуляторів, дозволяючи інженерам емпірично перевірити точність їхньої роботи на оригінальних системах [34].

Незалежно від обраної стратегії логічного збереження, фундаментальним рівнем будь-якого цифрового архіву залишається забезпечення фізичної надлишковості зберігання потоків бітів. Світова спільнота активно використовує архітектурний принцип LOCKSS (Lots of Copies Keep Stuff Safe - «Велика кількість копій зберігає речі в безпеці»), розроблений Стенфордським університетом. Цей принцип передбачає створення географічно та топологічно розподілених копій цифрових об'єктів у різних партнерських сховищах, які постійно здійснюють взаємний аудит цілісності. Якщо одна з копій пошкоджується через bit rot або кібератаку, система автоматично відновлює її з інших вузлів. Застосування LOCKSS доводить, що справжня цифрова стійкість досягається лише шляхом поєднання проактивної логічної трансформації з масштабною, децентралізованою фізичною надлишковістю [34].

Теоретичні моделі забезпечують концептуальний каркас архітектури, проте самі по собі не здатні гарантувати, що установа практично зможе підтримувати функціонування архіву протягом десятиліть. Для підтвердження інституційної здатності зберігати об'єкти необхідні суворі механізми вимірювання управлінської, фінансової та технологічної зрілості сховища. Головним інструментом у цій сфері є міжнародний стандарт ISO 16363:2012 «Аудит та сертифікація надійних цифрових сховищ» (Audit and certification of trustworthy digital repositories). Еволюціонувавши з попередніх проєктів RLG, NARA та критеріїв оцінки TRAC і DRAMBORA, цей стандарт надає вичерпну систему із понад сотні конкретних метрик. Він дозволяє зовнішнім незалежним аудиторам або внутрішнім комплаєнс-менеджерам глибоко аналізувати життєздатність установи [38].

Стандарт ISO 16363 розподіляє вимоги до цифрових сховищ на три основні категорії, кожна з яких вимагає від організації збору беззаперечної, формалізованої доказової бази (evidence) щодо ефективності її щоденних процедур.

У таблиці 1.2 представлено структурний та якісний аналіз цих категорій [38].

Категорія доказів	**Опис вимог та необхідної доказової бази**	**Значення для стабільності цифрового архіву**
Організаційна інфраструктура (Organizational Infrastructure)	Документальне підтвердження місії, фінансової стійкості, наявність детальних планів	Гарантує, що сховище не припинить існування через відсутність фінансування, і що дані

	безперервності бізнесу на випадок закриття (demise of the Archive), жорсткі політики заборони несанкціонованого видалення (ad-hoc deletions).	будуть передані наступникам.
Управління цифровими об'єктами (Digital Object Management)	Журнали процесів перетворення SIP на AIP (логування Інгесту), документація щодо планування збереження (моніторинг застарівання форматів).	Забезпечує технологічну здатність системи до подолання форматного застарівання.
Управління ризиками та безпекою (Risk Management and Security)	Дотримання стандартів кібербезпеки (серія ISO 27000), систематичний аудит апаратного/програмного забезпечення, фізичний захист ЦОД та логування доступу.	Формує стійкість до зовнішніх і внутрішніх загроз, унеможливлює витоки даних і руйнування архітектури внаслідок збоїв.

Табл. 1.2. Категорії аудиту та вимог до цифрових сховищ згідно з ISO 16363:2012 [38].

Отримання сертифікації за стандартом ISO 16363 є вкрай ресурсозатратним завданням. Провідні установи світу використовують його як орієнтир для розбудови своїх інфраструктур. Наприклад, Національне управління архівів та документації США (NARA), яке оперує понад мільярдом електронних файлів у понад 700 форматах, розробило стратегію цифрового збереження на 2022-2026 роки, безпосередньо спираючись на

вимоги надійності. Стратегія NARA передбачає масштабні цілі: опрацювання 85% архівних фондів, оцифрування 500 мільйонів сторінок до 2026 року, а також повну відмову від прийому паперових документів від федеральних агентств з червня 2024 року. Крім того, NARA документує конкретні плани дій щодо збереження форматів (Format Preservation Action Plans), мінімізуючи прийнятні типи файлів та впроваджуючи передові системи інтелектуального контролю [50].

Водночас для установ із меншими бюджетами або тих, що перебувають на початковому етапі цифрової трансформації, імплементація громіздкого ISO 16363 може стати непосильною перешкодою. Для вирішення цієї проблеми Коаліція цифрового збереження (DPC) розробила Модель швидкого оцінювання (Digital Preservation Coalition Rapid Assessment Model - DPC RAM), яка у 2024 році оновилася до версії 3.0. Вона дозволяє установам за короткий час (шляхом самооцінки) бенчмаркувати власні організаційні та сервісні можливості (від політик життєздатності до збереження бітстрімів) за п'ятибальною шкалою зрілості: від відсутності процесу до оптимізованого рівня. Важливою інновацією версії 3.0 стала інтеграція етичних норм та концепції «суверенітету даних корінних народів» (Indigenous data sovereignty), що перетворила компонент «Юридична база» на «Правові та етичні засади». Завдяки DPC RAM архіви отримують змогу візуалізувати розриви у своїх компетенціях за допомогою радарних діаграм та формувати покрокові дорожні карти безперервного покращення (Continuous Improvement) [27].

Не менш важливим світовим стандартом метрики є Рівні цифрового збереження Національного альянсу США (NDSA Levels of Digital Preservation). У новітній версії 2.1, випущеній у березні 2026 року, до матриці прийняття рішень було вперше інтегровано критерії екологічної стійкості

(environmental sustainability). Це означає, що відтепер стратегії надлишкового дублювання інформації (наприклад, LOCKSS) обмежуються і повинні враховувати вуглецевий слід та енергоефективність центрів обробки даних [51].

1.3. Інформаційна безпека, нормативно-правова база та цифровізація архівів в умовах воєнного стану в Україні

Проблема збереження даних тісно пов'язана з інформаційною безпекою, адже кібератаки можуть знищити архіви швидше, ніж застаріють формати файлів. Перетворення архівів на центри надання електронних послуг робить їх привабливими мішенями для програм-вимагачів (ransomware) та інших загроз. У цьому контексті дослідження Марченка В. підтверджує, що сучасне управління безпекою е-документів має інтегрувати правове регулювання, інституційні заходи та передові технічні засоби для захисту інфраструктур від крадіжок та несанкціонованої модифікації [44], [24], [40].

Саме тому в сучасному проєктуванні довірених цифрових сховищ необхідністю стало застосування таких підходів як «Безпека за замовчуванням» (Security by Design) та «Конфіденційність за замовчуванням» (Privacy by Design). Вони вимагають від системних інженерів інтегрувати багаторівневі механізми захисту на найраніших стадіях архітектурного задуму програмного забезпечення, а не встановлювати їх як патчі до вже функціонуючої і потенційно вразливої системи. Системний захист охоплює проактивність, превентивність, орієнтованість на користувача та абсолютну прозорість алгоритмів управління доступом. Законодавчо-нормативною основою розбудови таких систем виступають міжнародні стандарти інформаційної безпеки серії ISO/IEC 27000, які детально регламентують

вимоги до створення, впровадження, підтримки та постійного вдосконалення систем управління інформаційною безпекою (СУІБ) в установах [44], [40].

Надзвичайно важливим технологічним аспектом є управління криптографічними вразливостями баз даних, на яких базуються сучасні масштабні цифрові архіви. Зростання популярності нереляційних баз даних (NoSQL) для обробки петабайтних масивів неструктурованих метаданих та мультимедіа супроводжується специфічними викликами щодо управління ключами шифрування. Для забезпечення конфіденційності сенситивних фондів застосовується прозоре шифрування даних (Transparent Data Encryption, TDE) на рівні сховища (data at rest), а також інтеграція хмарних сервісів зберігання ключів (Key Vault). Проте, на рівні інженерних та фінансових компромісів, нативне шифрування створює нову проблему: воно унеможливлює подальшу дедуплікацію даних під час бекапу. Оскільки зашифровані блоки виглядають для систем як унікальний ентропійний шум, алгоритми не можуть виявити дублікати, що змушує архіви закуповувати значно більші обсяги фізичного дискового простору. Ця необхідність експоненційного розширення пам'яті є суворою, але необхідною фінансовою платою за гарантування конфіденційності [24], [40].

Крім того, згідно з фаховими настановами Національного інституту стандартів і технологій США (зокрема документом NIST SP 800-209), адміністраторам критично важливо розуміти значну різницю між резервним копіюванням та власним архівуванням. Резервне копіювання призначене для оперативного відновлення після локальних збоїв виробничих систем; такі копії активно оновлюються і швидко стають нерелевантними. Натомість архівування - це вилучення даних з активного обігу, переміщення їх у захищене середовище для тривалого зберігання та забезпечення їхньої абсолютної незмінності. Для захисту від програм-вимагачів, які здатні

знищити як оригінали, так і мережеві бекапи, архіви застосовують механізми кіберсховищ, створюючи «повітряний зазор» (air gap) між активною мережею та резервним фондом [24].

Управління ризиками для інституцій пам'яті в умовах кліматичних змін та воєнних загроз повинно спиратися на стандарт ISO 31000:2018, який визначає універсальні принципи ризик-менеджменту. У практичній діяльності архівісти застосовують матриці оцінки ризиків 5x5, розраховуючи критичність загрози як добуток її ймовірності на масштаб потенційних наслідків. Використання циклу Демінга (Plan-Do-Check-Act) забезпечує безперервність удосконалення СУІБ. Водночас аналітики застерігають щодо надмірного захоплення технологіями розподілених реєстрів: як зазначає Марченко В., хоча блокчейн може ефективно підтримувати цілісність реєстрів у короткостроковій перспективі, він є непридатним як субстрат для архівування з горизонтом понад 10 років через накопичення правових та криптографічних ризиків [39], [44].

В Україні активно тривають процеси цифровізації державних послуг, і сфера діловодства та архівної справи проходить через стадію масштабної модернізації. Розвиток національного цифрового архівування зумовлений трьома паралельними стратегічними процесами: глибокою потребою в інтеграції з європейським цифровим простором, жорсткими вимогами кібербезпеки та іншими викликами, пов'язаними з воєнним станом і загрозою фізичного знищення інфраструктури внаслідок збройної агресії [8], [15], [13], [3].

Фундамент правового регулювання галузі складають базові Закони України «Про Національний архівний фонд та архівні установи» та «Про електронні документи та електронний документообіг». Ці акти закріплюють презумпцію юридичної рівнозначності електронних і паперових документів,

чітко регламентуючи, що терміни зберігання електронних записів не можуть бути меншими за терміни, встановлені для їхніх паперових аналогів.

Життєво важливою складовою забезпечення доказової сили таких архівів є Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (закон отримав нову назву у зв'язку з євроінтеграційними процесами). Він не лише регламентує використання кваліфікованих електронних підписів (КЕП), але й закладає правове підґрунтя для імплементації новітнього Регламенту (ЄС) 2024/1183 (відомого як eIDAS 2.0), що набув чинності у травні 2024 року. Згідно зі статтями 45g-45j цього Регламенту, електронне архівування офіційно визнано кваліфікованою довірчою послугою. Це правова революція: електронні документи, що зберігаються з використанням такого кваліфікованого сервісу, тепер автоматично наділяються презумпцією цілісності та незмінності походження на весь період їх збереження, що унеможливлює відхилення їх судами виключно через електронну форму [30] [4].

Важливим кроком до оновлення термінологічної бази стало прийняття у 2023 році національного стандарту ДСТУ 2732:2023 «Діловодство й архівна справа. Терміни та визначення понять», який остаточно набув чинності 1 березня 2024 року, скасувавши застарілі норми 2004 року. Цей стандарт легалізував в українському правовому полі сучасний понятійний апарат європейського зразка, концептуалізувавши поняття «електронного архіву» та структурувавши процеси передавання документів на архівне зберігання [8], [15], [13].

На інституційному рівні флагманом галузі у публічному секторі виступає Центральний державний електронний архів України (ЦДЕАУ), що забезпечує довготривале зберігання електронних документів вищих державних органів та формує політику диференційованого доступу. Під

стратегічним керівництвом Міністерства юстиції та Державної архівної служби в державі активно розгортається масштабна урядова ініціатива - проєкт «е-Архів». Цей проєкт спрямований на автоматизацію життєвого циклу документів, що від самого початку були створені в електронній формі (born-digital), унеможливлюючи їх втрату на критичному етапі міжвідомчої передачі. Концептуальна мета проєкту полягає у розбудові розгалуженої мережі галузевих електронних архівів, що будуть об'єднані єдиним національним центром обробки даних (ЦОД) з високим рівнем кіберзахисту [19], [15], [13].

Паралельно комерційний сектор IT динамічно інтегрується з державними інституціями, пропонуючи потужні хмарні рішення для корпоративного ринку. Платформи електронного документообігу, як-от Vchasno.EDO, надають бізнесу послуги безлімітних електронних архівів, що базуються на розподілених глобальних інфраструктурах на кшталт Amazon Web Services (AWS). У таких системах клієнтські дані проходять обов'язкове криптографічне шифрування за сучасними протоколами ще на локальному рівні, до моменту завантаження файлу в хмарне сховище, що гарантує цілісність інтелектуальної власності [11].

В академічному та бібліотечному секторах України також тривають дослідження ефективності використання протоколів масового обміну метаданими. Для агрегації величезних масивів розпорошених наукових даних вітчизняні фахівці успішно впроваджують цифрову платформу VuFind як основу для розбудови ETL-архітектури (Extraction, Transformation, Loading). Дослідження Новицького О. доводять, що завдяки підтримці протоколу OAI-PMH (Open Archives Initiative Protocol for Metadata Harvesting), установи здатні автоматично збирати розрізнені метадані з університетських репозитаріїв та цифрових бібліотек, приводячи їх до єдиного стандарту для

зручного пошуку. Водночас інший дослідник, Моджада Г., зазначає, що оскільки OAI-PMH не має жорстких вимог до семантичної структури даних (що призводить до труднощів з інтеграцією повнотекстових матеріалів і відсутності оновлень у реальному часі), успішна інтеграція вимагає застосування додаткових інструментів, мапінгу даних і переходу на гібридні підходи [55], [49].

Повномасштабне вторгнення російської федерації стало жорстоким, але надзвичайно потужним каталізатором для прискореного розгортання цифрових архівів. Фізичне знищення музеїв, університетів і сховищ у зонах бойових дій вимагало від українського уряду миттєвої реакції у вигляді масового оцифрування фондів для збереження української історичної пам'яті.

Проте такі масштабні ініціативи оцифрування зіштовхуються з серйозними нормативними колізіями. Згідно зі статтею 22 Закону України «Про авторське право і суміжні права», бібліотеки та архіви мають право на вільне репрографічне відтворення (копіювання) одного примірника твору виключно з метою збереження фондів, які руйнуються. Проте ця норма не надає їм прямого права публікувати такі цифрові копії у відкритий онлайн-доступ (особливо це стосується «сирітських творів»), що створює ризик фінансових позовів за порушення майнових прав. Додатковим викликом є Закон України «Про захист персональних даних» та європейський регламент GDPR. На практиці виникає жорсткий концептуальний конфлікт між правом суб'єкта на стирання даних («правом на забуття») та суспільним інтересом у збереженні історії. Хоча частина 8 статті 6 Закону України допускає подальшу обробку персональних даних в історичних чи наукових цілях , вона категорично вимагає від цифрових архівів розгортання систем суворого технічного захисту, псевдонімізації та обмеження несанкціонованого публічного доступу до чутливої інформації [12] [14].

У таблиці 1.3 наведено показники посилення процесів цифровізації державних архівів України [18], [15], [3].

Показники та цілі	**Статистичні дані та динаміка розвитку**
Зростання загальних обсягів оцифрованих фондів	Збільшення кількості оцифрованих документів на 63,5% за короткий період із загальним обсягом понад 8,5 млн збережених одиниць.
Продуктивність процесів цифровізації	Протягом 2023 року архівістами створено понад 21 млн цифрових копій документів. План на 2024 рік становить щонайменше 30 млн копій. Систему підтримують понад 50 операторів, кожен з яких генерує близько 2000 копій щодня.
Структура збережених цифрових масивів інформації	Текстові архівні матеріали становлять 45%, історичні фотографії - 30%, аудіодокументи - 15%, відеохроніки - 8%, інтерактивні мультимедіа - 2%.
Користувацький попит, доступність та ШІ-навігація	Зафіксовано стрімке зростання кількості онлайн-запитів до е-архівів на 106,7% (понад 3,1 млн звернень громадян та науковців на рік). Застосування штучного інтелекту для розпізнавання текстів підвищило швидкість і релевантність пошуку на 70%.

Табл. 1.3. Показники динаміки цифровізації архівів України (2023-2024) [3].

Як переконливо свідчать статистичні дані, український досвід масштабного оцифрування та використання технологій хмарного зберігання в

умовах знеструмлень та ракетних обстрілів отримав значне визнання міжнародної спільноти. Делегації країн ЄС (зокрема Естонії) активно переймають український досвід забезпечення цифрової стійкості інституцій. В Україні електронний архів остаточно перетворився з допоміжного інструмента бюрократичної оптимізації на стратегічний елемент національної безпеки, інформаційного суверенітету та гарантування збереженості історичної пам'яті нації [18], [3].

ВИСНОВКИ ДО РОЗДІЛУ 1

Проведене дослідження теоретичних засад та практичних аспектів розбудови систем управління електронними архівами дозволяє сформулювати низку вагомих стратегічних висновків.

Загроза безповоротної втрати світової інтелектуальної спадщини через апаратно-програмне застарівання є доведеним емпіричним фактом. Гіпотеза «цифрових темних віків» знаходить підтвердження у статистиці, згідно з якою понад 27% сучасних наукових публікацій перебувають під загрозою зникнення через відсутність належного архівування. Цифрові об'єкти відрізняються надзвичайною вразливістю і вимагають проактивних, фінансово забезпечених втручань протягом усього свого життєвого циклу. Просте зберігання файлів на серверах або присвоєння DOI не вирішує проблеми деградації контенту.

Впровадження міжнародних еталонних моделей, насамперед архітектурного стандарту OAIS (ISO 14721) та систем метаданих PREMIS v3.0, є єдиним шляхом до створення надійних цифрових архівів. Суворий концептуальний розподіл інформаційних пакетів на SIP, AIP та DIP, поєднаний із дотриманням принципу криптографічної незмінності об'єктів під час міграції чи емуляції, створює бездоганний ланцюжок довізного

контролю та зберігає юридичну силу документів. Паралельне впровадження принципу географічної надлишковості LOCKSS гарантує фізичне виживання потоків бітів у разі локальних катастроф.

Практична оцінка надійності цифрових сховищ вимагає застосування жорстких критеріїв. Використання стандарту аудиту ISO 16363 та моделі швидкої оцінки зрілості DPC RAM (включно з її етичними аспектами суверенітету даних) дозволяє інституціям виявляти вразливості та планувати безперервний розвиток. Зростання кількості кібератак, зокрема програм-вимагачів, зобов'язує розробників впроваджувати концепції Security by Design, прозоре шифрування баз даних, а також жорстко розмежовувати процеси оперативного резервного копіювання та довгострокового архівування з використанням повітряних зазорів. Управління ризиками відповідно до ISO 31000 стає щоденною необхідністю для архівних адміністраторів.

Україна демонструє вражаючу здатність до цифрової стійкості та адаптації інституцій в умовах збройного конфлікту. Синхронізація нормативної бази (через прийняття ДСТУ 2732:2023), реалізація національного проєкту «е-Архів» і успішне розгортання академічних систем збирання метаданих (VuFind за протоколом OAI-PMH) доводять високу технологічну зрілість вітчизняного державного сектору.

В умовах повномасштабної війни, коли оцифровано десятки мільйонів копій архівних документів, цифровізація стала не просто засобом адміністративної оптимізації, а необхідною умовою для збереження державної ідентичності, культурної спадщини та національної пам'яті для майбутніх поколінь.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ЦИФРОВОГО АРХІВУВАННЯ У ДЕРЖАВНОМУ АРХІВІ РІВНЕНСЬКОЇ ОБЛАСТІ

Широка цифровізація трансформує діяльність архівних установ. Враховуючи загрози втрати електронних ресурсів через застарівання форматів, а також прямий вплив бойових дій на території України, виникає нагальна потреба в розбудові надійних систем збереження даних на регіональному рівні. Цей розділ присвячено аналізу процесів архівації на прикладі Державного Рівненської архіву області.

В умовах війни на території України ці технологічні виклики доповнюються загрозами фізичного знищення національної документальної пам’яті. Такі обставини вимагають від держави максимального посилення процесів цифровізації та створення надійних систем електронного збереження, здатних протистояти як кінетичним, так і кібернетичним ударам.

З огляду на необхідність імплементації міжнародних моделей, зокрема OAIS та стандартів аудиту надійних цифрових сховищ, цей розділ присвячено аналізу системи процесів цифрового архівування на базі Державного архіву Рівненської області. Дослідження структурно-функціональної організації установи, оцінка технологічних потужностей сектору інформаційних технологій, аналіз методів управління фондами та виявлення вразливостей в архітектурі збереження дозволяють сформувати картину готовності регіональних інституцій пам’яті до функціонування в умовах сучасних інформаційних та безпекових викликів [37].

2.1. Загальна характеристика діяльності та інституційна роль Державного архіву Рівненської області

Державний архів Рівненської області є науково-дослідною та інформаційною установою, що входить до системи архівної справи України. Діяльність цього інституту спрямована на безпосередню реалізацію державної політики у сфері архівної справи та діловодства на підвідомчій території, що робить його важливим елементом механізму збереження національної ідентичності та інституційної пам’яті. В умовах сучасних інформаційних трансформацій архів еволюціонував від традиційного пасивного сховища паперових артефактів до складного технологічного центру. Цей центр покликаний регулювати життєвий цикл документальної інформації від моменту її створення в установах-фондоутворювачах до етапу електронного збереження або знищення [2].

Головною місією установи є забезпечення неперервності документальної пам’яті регіону шляхом включення документів до Національного архівного фонду (НАФ), їх систематизації та створення належних умов для постійного збереження. Ця місія реалізується через діяльність, яка охоплює як суто архівні, так і наглядово-регуляторні функції.

Одним із пріоритетних завдань архіву є управління архівною справою та координація роботи як державних, так і приватних архівних установ, що функціонують на території області. Такий підхід дозволяє формувати єдиний правовий та технологічний простір діловодства, гарантуючи застосування стандартизованих методик обробки документів незалежно від форми власності установи, яка їх створює [16].

Реалізація державної політики нерозривно пов’язана із забезпеченням конституційного права громадян на інформацію. Тому стратегічним напрямом діяльності архіву є гарантування вільного та прозорого доступу суспільства до публічної інформації, що зберігається в його фондах. Цей аспект набуває особливої актуальності в контексті загальнодержавного оцифрування, коли

доступність вимірюється не лише відкритістю читальних залів, але й наявністю оцифрованих довідкових апаратів та електронних копій документів у глобальній мережі. Відповідно до цього, установа активно залучена до проведення наукових досліджень у галузі архівознавства та документознавства, що створює підґрунтя для імплементації новітніх технологій у щоденну практику збереження [10].

Окремим і надзвичайно важливим блоком завдань є контрольно-наглядова діяльність. Державний архів Рівненської області здійснює систематичний контроль за діяльністю служб діловодства в регіональних органах виконавчої влади, органах місцевого самоврядування та на підприємствах, перевіряючи дотримання ними державних стандартів. Зокрема, ключовим регуляторним орієнтиром є дотримання вимог стандарту ДСТУ 2732:2023, який уніфікує термінологічну базу в роботах зі стандартизування та управління документацією [11].

Цей превентивний контроль є критично необхідним, оскільки саме на етапі поточного діловодства закладається основа майбутнього архівного фонду; втрата або неправильне оформлення документів в установі-творці унеможливлює їх подальше історичне збереження. Водночас, в умовах тотальної цифровізації, архів бере на себе відповідальність за захист персональних даних та інформації з обмеженим доступом, що вимагає впровадження складних протоколів інформаційної безпеки.

Функціональний апарат Державного архіву Рівненської області є глибоко диверсифікованим. До основних функцій належить довгострокове збереження, консервація та фізична реставрація історичних документів, що забезпечує зупинення процесів природної деградації матеріальних носіїв. Стратегічним напрямом, особливо в умовах воєнного стану, є формування копій для страхового фонду, що гарантує збереження змісту унікальних

документів у разі незворотного фізичного знищення оригіналів. Окрім того, установа здійснює прийом документації від юридичних та фізичних осіб для внесення до НАФ, проводить експертизу цінності та забезпечує систематизацію отриманих матеріалів [16].

Основні напрями діяльності архіву наведено в таблиці 2.1.

Група функцій	**Змістовне наповнення функцій**	**Значення для стабільності інституційної пам'яті**
Комплектування та експертиза	Прийом документів, систематизація фондів, проведення експертизи цінності, відбір документів до НАФ.	Формує документальну базу національної історії, гарантуючи, що жоден значущий документ не буде втрачений.
Збереження та реставрація	Довгострокове збереження, консервація, фізична реставрація історичних документів. Формування копій для страхового фонду.	Забезпечує фізичне виживання оригіналів. Створення страхового фонду є фундаментальним механізмом захисту від втрат.
Довідково-комунікаційна	Обслуговування користувачів у читальних залах, видача довідок, надання копій документів, забезпечення вільного	Забезпечує реалізацію прав громадян, підтримує історичні дослідження, слугує доказовою базою для підтвердження юридичних фактів.

	доступу до публічної інформації.	
Наглядово-регуляторна	Інспектування архівних підрозділів та служб діловодства інших установ області. Надання методичної підтримки.	Формує єдиний правовий простір діловодства в регіоні. Запобігає несанкціонованому знищенню документів на етапі відомчого зберігання.
Цифровізація та інновації	Автоматизація обліку документів, оцифрування фондів, інтеграція з пошуковими системами.	Мінімізує фізичний знос оригіналів, радикально розширює географію доступу до документів, інтегрує архів у міжнародний простір.

Таблиця 2.1. Функціональна матриця діяльності Державного архіву Рівненської області [5].

Таким чином, Державний Рівненської архів області виконує не лише функцію ретроспективного збереження документів, а й бере участь у координації процесів діловодства в регіоні. Його інституційна спроможність напряму залежить від успішного впровадження інноваційних технологій збереження. Успішне виконання архівних функцій сьогодні залежить не лише від наявності фізичних площ для зберігання справ, але й від здатності установи ефективно модернізувати внутрішні діловодні процеси, впроваджувати інформаційні технології та будувати надійні системи, здатні протистояти технологічному застаріванню та кіберзагрозам.

2.2. Оцінка організації процесів цифровізації та апаратно-мережевої архітектури

Ефективність функціонування будь-якої сучасної архівної установи визначається рівнем організації її внутрішніх управлінських та технологічних процесів. У Державному архіві Рівненської області система діловодства та управління ресурсами становить складний багатокомпонентний механізм. Найважливішим структурним підрозділом у контексті цієї роботи є сектор інформаційних технологій, оцифрування та реставрації документів, який відповідає за практичну імплементацію концепції цифрового архівування.

Оцінка діяльності цього сектору дозволяє виявити глибокі протиріччя між амбітними завданнями з оцифрування та обмеженнями реального ресурсного забезпечення. Відповідно до результатів практики, основними проблемами установи є критичний дефіцит кадрів та застаріла матеріально-технічна база, яка включає сервери та спеціалізовані сканери.

Кадровий голод не входить у тему даного дослідження, тому вся увага буде приділена технічним аспектам.

Спираючись на міжнародну еталонну модель OAIS, процес переведення паперових артефактів у цифровий формат слід розглядати як етап «Приймання» (Ingest). Під час цього етапу фізичний документ конвертується в Інформаційний пакет подання (Submission Information Package - SIP). Цей процес вимагає надзвичайної точності, обережного поводження зі старовинними документами та значних технологічних потужностей.

Пріоритетним напрямом для оцифрування у архіві є метричні книги (наприклад, фонди Р-740 та Р-204), оскільки вони мають найбільший попит серед громадян та дослідників-генеалогів. Масове сканування таких об'єктів генерує величезні масиви неструктурованих даних, управління якими вимагає

чіткої політики форматів та структурованих метаданих [6].

Після створення SIP, система повинна сформувати Архівний інформаційний пакет (Archival Information Package - AIP), який є майстер-копією, призначеною для довгострокового або вічного збереження. Згідно зі стандартами цифрового збереження, розробленими ініціативою FADGI (Federal Agencies Digital Guidelines Initiative) та NDSA (National Digital Stewardship Alliance), для AIP повинні використовуватися формати, що не застосовують стиснення з втратами (так звані lossless formats). Стандартом у світовій практиці є нестиснений формат TIFF або алгоритми JPEG 2000 Lossless (.jp2) [53].

Бібліотека Конгресу США (Library of Congress) прямо вказує на нестиснений TIFF як на пріоритетний формат для архівних майстер-копій візуальних матеріалів, оскільки він має простішу внутрішню структуру та ширшу підтримку інструментарієм довгострокового збереження [53].

Робочим форматом оцифрування наразі є переважно JPEG. IT-фахівці установи усвідомлюють та визнають технологічні переваги формату TIFF для створення майстер-копій, які не втрачають якості при багаторазовому використанні, проте масовий перехід на нього ускладнюється жорсткими обмеженнями дискового простору та ресурсів. Формат JPEG використовує алгоритми дискретного косинусного перетворення (DCT), що призводять до незворотної втрати піксельної інформації (lossy compression). Кожне перезбереження або міграція файлів у форматі JPEG на нові платформи незворотно знищуватиме частину візуальних даних, призводячи до явища кумулятивної генераційної деградації [41].

Збереження AIP у форматі JPEG є порушенням фундаментального принципу незмінності та достовірності архівних доказів.

Функція забезпечення доступу (Access) в моделі OAIS реалізується

через генерацію Інформаційних пакетів розповсюдження (Dissemination Information Package - DIP) [37].

Для цілей публікації на офіційному вебсайті та передачі користувачам відскановані зображення конвертуються у багатосторінковий формат PDF. Це рішення є прагматичним та відповідає загальноприйнятим практикам зручності користувачів, оскільки PDF (зокрема PDF/A) широко підтримується всіма операційними системами.

Проте архітектура дистрибуції цих даних містить суттєві обмеження. Сервер, де розміщений сайт архіву розміщений віддалено у дата-центрі в Києві, а квота на зберігання даних для архіву жорстко обмежена до 500 ГБ. Враховуючи, що регіональні архіви оперують мільйонами скан-копій, обсяг у 500 ГБ є критично недостатнім для розгортання повноцінного онлайн-каталогу з можливістю перегляду зображень високої роздільної здатності.

Через ці інфраструктурні обмеження установа змушена використовувати комерційні сервіси для виконання своїх статутних обов'язків з обслуговування громадян. Замовникам надається тимчасовий доступ (до 6 місяців) до цифрових копій через сервіс Google Drive. З точки зору інформаційної безпеки та міжнародних стандартів, таких як ДСТУ EN ISO/IEC 27037:2022 щодо збирання та збереження цифрових доказів, використання споживчих хмарних платформ загального призначення (Public Cloud) створює низку юридичних та технічних ризиків. Google Drive не гарантує довгострокової незмінності файлів, не генерує надійні журнали аудиту доступу та метадані ланцюга постачання (chain of custody), які необхідні для підтвердження автентичності документа [9].

Стратегічним напрямом вирішення цієї проблеми є інтеграція архіву у масштабні загальнонаціональні інформаційні системи. Ключовим кроком у

розвитку є міжархівний пошуковий портал «Архіум» (Archium), розроблений приватним підприємством «Архівні інформаційні системи» за ініціативи Державної архівної служби України. Ця платформа об'єднує в єдиному пошуковому просторі електронні ресурси центральних та обласних архівів, налічуючи десятки мільйонів цифрових зображень. Інтеграція масивів Державного архіву Рівненської області до порталу «Архіум» дозволяє делегувати завдання хостингу петабайтів даних та забезпечення безперебійного доступу спеціалізованій національній інфраструктурі, ліквідуючи залежність від обмеженої квоти у 500 ГБ та невідповідних споживчих сервісів типу Google Drive [1].

У таблиці 2.2 наведено результати аналізу відповідності процесів архівування моделі OAIS

Етап	**Теоретичні вимоги**	**Поточна реалізація в установі**	**Оцінка відповідності**
Ingest (Приймання)	Генерація SIP, перевірка якості сканування, формування технічних метаданих.	Масове сканування метричних книг. Формування файлів без метаданих (PREMIS).	Часткова відповідність. Дефіцит кадрів призводить до пропусків у контролі якості.
Archival Storage (Збереження)	Створення майстер-копій (AIP) у нестиснених форматах	Використання формату JPEG для економії місця. Зберігання на	Невідповідність. Стиснення з втратами гарантує деградацію

	(TIFF/JPEG 2000 Lossless). Забезпечення побітової цілісності.	локальному NAS без бекапів.	якості. Відсутність резервування загрожує втратою даних.
Access (Доступ)	Генерація DIP. Надання зручного інтерфейсу пошуку. Аудит доступу.	Конвертація у PDF. Хостинг на власному сайті (ліміт 500 ГБ) та використання Google Drive. Інтеграція з платформою «Архіум».	Низька зрілість власної інфраструктури, проте напрям на підключення до національних систем (Архіум) є стратегічно правильним.

Таблиця 2.2. Аналіз відповідності процесів архівування моделі OAIS

Фізичне збереження згенерованих цифрових масивів та забезпечення їхньої доступності для співробітників архіву базується на мережевій інфраструктурі та серверному обладнанні. Аналіз топології мережі та систем зберігання даних дозволяє оцінити рівень кіберстійкості установи відповідно до вимог серії стандартів ISO/IEC 27000 щодо систем управління інформаційною безпекою [40].

Інфраструктура архіву, що налічує близько 40 робочих станцій, розподілена між двома корпусами. Критичним недоліком мережевої архітектури є використання пласкої топології. Відсутність віртуальних локальних мереж (VLAN) або мікросегментації означає, що всі пристрої установи перебувають в одному широкомовному домені.

У контексті сучасної кібербезпеки концепція пласкої мережі розглядається як критична вразливість, що порушує принцип ешелонованої

оборони (Defense in Depth). Пласка мережа функціонує як магістраль для діяльності зловмисників та шкідливого програмного забезпечення. Якщо робоча станція будь-якого співробітника (наприклад, у канцелярії або читальному залі) буде скомпрометована через фішинговий лист або експлуатацію вразливості в браузері, відсутність сегментації дозволить шкідливому ПЗ безперешкодно сканувати всі IP-адреси в мережі. У такій архітектурі шкідливе ПЗ може вільно звертатися до портів управління серверами або протоколів обміну файлами (SMB/NFS) на критичних вузлах. При використанні мікросегментації трафік між робочими станціями та серверами за замовчуванням блокується і дозволяється лише за необхідності. Натомість пласка топологія архіву робить сховища даних настільки ж вразливими, наскільки вразливим є будь-який комп'ютер у мережі [69], [47], [71].

Ситуація ускладнюється децентралізованою системою управління доступом. Технічний аудит фіксує повну відсутність служби каталогів (Active Directory або її аналогів). Це означає, що ідентифікація, автентифікація та авторизація користувачів здійснюються локально на кожній окремій машині. Відповідно до вимог стандарту ISO/IEC 27001, відсутність централізованої ідентифікації суттєво підвищує вразливість системи. Адміністратор фізично не здатний централізовано впровадити політики складності паролів, примусову їх зміну, блокування облікових записів після серії невдалих спроб входу або обов'язкову багатофакторну автентифікацію (MFA) для доступу до корпоративних ресурсів. Більше того, розрізнені облікові записи сприяють використанню слабких паролів та полегшують атаки типу вилучення облікових даних з пам'яті (OS Credential Dumping), що вкрай небезпечно для інституції, яка зберігає конфіденційні матеріали [7], [46].

Збереження цифрових архівів, що відповідає етапу Archival Storage за

моделлю OAIS, в установі забезпечується використанням мережевого накопичувача (NAS) виробництва компанії Synology. Конфігурація дискової підсистеми розділена на два логічні томи:

1. Том 1: масив RAID 5, побудований на жорстких дисках об'ємом 3 ТБ кожен. Цей масив, очевидно, використовується для поточних робочих процесів оцифрування [70].
2. Том 2: масив із надмірністю (ймовірно RAID 1 або пропрієтарна технологія Synology Hybrid RAID - SHR), побудований на двох накопичувачах об'ємом по 10 ТБ, доступ до якого жорстко обмежений і надається виключно системному адміністратору [70].

Схему роботи RAID 1 можна побачити на рис. 2.1.

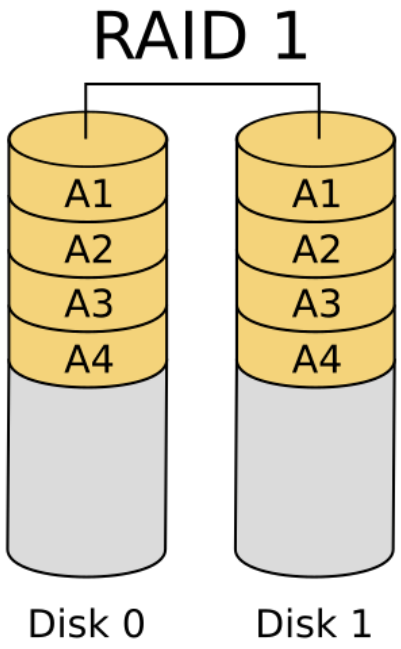


рис. 2.1. Схема роботи RAID 1 [70]

Схему роботи RAID 5 можна побачити на рис. 2.2.

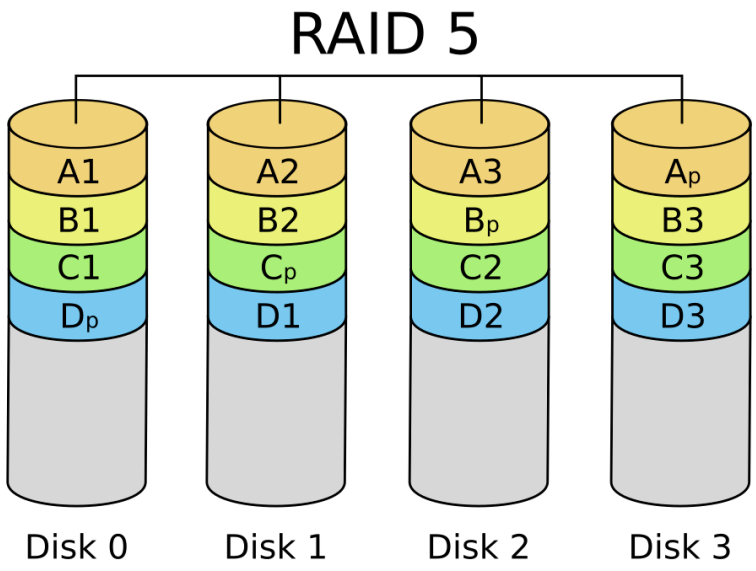


рис. 2.2. Схема роботи RAID 5 [70]

Хоча використання масивів з апаратною надмірністю (RAID) є стандартом індустрії для забезпечення безперервності бізнес-процесів, така архітектура несе приховані ризики без належного інженерного супроводу. Зокрема, використання архітектури RAID 5 на масивах з дисками ємністю 3 ТБ створює серйозну загрозу безповоротної втрати даних через проблему невідновлюваних помилок читання (Unrecoverable Read Error - URE).

Природа цієї проблеми полягає в тому, що жорсткі диски споживчого та напівпрофесійного класу (SATA) мають заявлений виробником рейтинг помилок читання. Це означає, що статистично один із **10^14** прочитаних біт буде нечитабельним через мікродефекти магнітного покриття. У нормальному режимі роботи RAID-контролер виправляє ці помилки на льоту, використовуючи блоки парності. Проте, коли один диск у масиві RAID 5 виходить з ладу, масив переходить у деградований стан (Degraded Mode). Для відновлення даних (rebuild / resilvering) на новий диск, контролер зобов'язаний прочитати кожний сектор на всіх дисках, що залишилися [67], [35].

Помилка URE під час ребілду масиву зупиняє процес і призводить до виходу з ладу всього логічного тому RAID 5, спричиняючи втрату даних. Через цей структурний недолік використання RAID 5 для масивів з дисками великої ємності вважається ризикованим; сучасні індустріальні стандарти вимагають переходу на архітектури з подвійною надмірністю, такі як RAID 6 або RAID 10 [66].

Другою проблемою архітектури зберігання є Bit Rot, описаний у розділі 1. Дані на магнітних дисках здатні поступово деградувати через ослаблення магнітних доменів, космічне випромінювання або дрібні помилки в прошивці контролерів [42].

Оскільки немає даних про використання сучасних файлових систем з функцією Copy-on-Write (CoW), таких як Btrfs, можна припустити використання стандартної для Synology системи ext4.

Проблема полягає в тому, що файлова система ext4 не зберігає контрольних сум (checksums) для самих даних (лише для метаданих) і не здатна виявляти апаратні пошкодження файлів. Якщо фізичний біт інвертується на диску, операційна система просто зчитає і передасть користувачу пошкоджений файл без жодного попередження. Для архіву, який зберігає візуальні копії історичних документів, це означає, що пікселі в зображеннях можуть деградувати роками (цифрове розкладання), поки хтось випадково не відкриє файл і не виявить незворотні артефакти або неможливість декодування [62], [54].

У таблиці 2.3. наведено кількісні та якісні показники інфраструктури архіву та їх критичність

Компонент інфраструктури	**Фактичний стан**	**Аналітичне значення для безпеки системи**

Топологія локальної мережі	Єдина пласка мережа, ~40 вузлів без VLAN.	Критична вразливість. Сприяє вільному переміщенню шкідливого ПЗ між робочими станціями та серверами.
Централізоване управління	Відсутня (децентралізоване управління).	Неможливість централізованого впровадження політик паролів та багатофакторної автентифікації (MFA). Ризик крадіжки облікових даних.
Архітектура зберігання даних	Том 1: RAID 5 (3 ТБ диски). Том 2: SHR/RAID 1 (10 ТБ диски).	Том 1 перебуває в зоні високого ризику краху під час ребілду через URE. Відсутність згадки про файлову систему Btrfs або ZFS вказує на вразливість до деградації даних.

Таблиця 2.3. Кількісні та якісні показники інфраструктури архіву та їх критичність

2.3. Системний аналіз вразливостей в політиках резервного копіювання та моніторингу

Головною вразливістю IT-інфраструктури Державного архіву Рівненської області є повна відсутність системи резервного копіювання. Оскільки унікальні дані зберігаються виключно в єдиному екземплярі на локальному накопичувачі NAS, будь-який апаратний збій або атака

вірусу-вимагача може призвести до безповоротної втрати інформації. Політики зовнішнього доступу та моніторингу носіїв також потребують доопрацювання.

Цей факт свідчить про порушення міжнародних стандартів надійного цифрового зберігання (зокрема, принципів LOCKSS).

Світовим стандартом індустрії інформаційних технологій є дотримання стратегії резервного копіювання «3-2-1». Це правило вимагає створення та підтримки як мінімум трьох копій даних (однієї основної та двох резервних), які зберігаються на носіях двох різних типів, причому одна з копій обов'язково повинна зберігатися поза межами основного офісу (off-site) або в хмарному середовищі. В умовах воєнного стану, коли установи перебувають під постійною загрозою ракетних обстрілів, відключень електроенергії та фізичного пошкодження центрів обробки даних, відсутність географічно віддалених (офлайн) копій є фатальною помилкою [22].

Використання RAID-масивів на NAS створює фальшиве відчуття безпеки. Необхідно чітко розмежовувати поняття відмовостійкості та резервного копіювання. Архітектура RAID захищає виключно від механічної поломки одного або декількох жорстких дисків. Вона безпорадна перед такими загрозами, як випадкове видалення директорії, логічне пошкодження файлової системи через стрибок напруги, навмисна дія інсайдера або, що найактуальніше, умисне шифрування даних програмою-вимагачем.

Будь-яка деструктивна зміна даних на масиві миттєво реплікується на всі дзеркальні диски, безповоротно знищуючи оригінали.

Внутрішній захист спирається на використання системи Cisco Umbrella, яка забезпечує фільтрацію запитів на рівні DNS і блокує переходи на відомі шкідливі домени. Хоча це корисний механізм для протидії базовим фішинговим кампаніям, його недостатньо для стримування складних

цілеспрямованих атак [25].

Установа знаходиться в процесі підключення до платформи MISP (Malware Information Sharing Platform). MISP є стандартом де-факто для обміну індикаторами компрометації (Indicators of Compromise - IoC), такими як шкідливі IP-адреси, фішингові домени, хеші файлів та шаблони атак у форматі STIX/TAXII. Вона дозволяє агрегувати розвідувальну інформацію про загрози (Threat Intelligence) від партнерів (наприклад, CERT-UA або НАТО) [48], [68].

Однак, архітектурна проблема полягає в тому, що MISP сама по собі не є активним засобом захисту - це розширена база знань. Без належної автоматизації та інтеграції MISP з активними системами виявлення вторгнень (IDS/IPS), корпоративними файрволами (NGFW) або системами управління подіями безпеки (SIEM), ефективність платформи зводиться до мінімуму. У поточному стані інфраструктури архіву, де відсутня глибока аналітика трафіку, інтеграція з MISP ризикує залишитися формальною процедурою: аналітикам доведеться вручну перевіряти індикатори, що унеможливлює оперативне реагування на автоматизовані загрози [45].

У таблиці 2.4. продемонстрована матриця кіберризиків та порушень політик безпеки

Категорія вразливості	**Сутність проблеми в інфраструктурі**	**Потенційні наслідки (Ризики)**	**Теоретично обґрунтовані механізми нейтралізації**
Резервне копіювання	Ігнорування правила «3-2-1». Дані в	Тотальна і незворотна втрата даних у	Застосування «кіберсховищ» з повітряним

	єдиному екземплярі на локальному NAS.	разі апаратного краху, пожежі або атаки.	зазором. Вивантаження бекапів у хмарні ЦОД.
Threat Intelligence	Підключення до MISP без інструментів автоматичного реагування (SIEM/NGFW).	Платформа працюватиме як пасивна база; аналітики не зможуть блокувати загрози в реальному часі.	Інтеграція REST API MISP з активним мережевим обладнанням для автоматичного блокування індикаторів компрометації.
Моніторинг носіїв	Виключно реактивна заміна дисків після відмови (повідомлення від ОС Synology).	Несподіваний вихід з ладу дисків під навантаженням; ризик каскадної відмови під час ребілду.	Проактивний моніторинг S.M.A.R.T. та використання систем предиктивної аналітики деградації пластин.

Таблиця 2.4. Матриця кіберризиків та порушень політик безпеки

ВИСНОВКИ ДО РОЗДІЛУ 2

Проведений аналіз системи цифрового архівування Державного архіву Рівненської області дозволяє зробити висновок, що установа є ключовим центром збереження національної інституційної пам'яті, який перебуває на етапі складної трансформації з традиційного сховища у технологічний центр. Незважаючи на активне переведення документів у цифровий формат, інфраструктура архівування має низку критичних невідповідностей міжнародним стандартам та моделі OAIS.

Зокрема, процеси оцифрування супроводжуються серйозними порушеннями принципів збереження даних: через брак дискового простору майстер-копії створюються у форматі JPEG зі стисненням із втратами замість нестисненого формату TIFF, що неминуче призводить до кумулятивної генераційної деградації архівних документів. Жорсткі обмеження хостингу (лише 500 ГБ) змушують архів використовувати для дистрибуції матеріалів споживчі хмарні сервіси загального призначення (Google Drive), які не гарантують незмінності файлів і необхідного аудиту, хоча стратегічно правильним кроком визначено майбутню інтеграцію з національним порталом «Архіум».

Аналіз апаратно-мережевої архітектури виявив вразливості системи кібербезпеки: локальна мережа є пласкою (без VLAN та сегментації), що сприяє вільному поширенню шкідливого програмного забезпечення, а відсутність централізованої служби каталогів (Active Directory) створює високі ризики компрометації облікових даних. У системах зберігання даних використання застарілої архітектури RAID 5 на масивах із великими дисками загрожує повною втратою інформації через невідновлювані помилки читання (URE), тоді як відсутність файлових систем із підтримкою контрольних сум робить масиви вразливими до «тихого» пошкодження файлів.

Найбільш критичною прогалиною, що несе серйозну загрозу для цифрових фондів, є повна відсутність системи резервного копіювання та ігнорування стандарту «3-2-1». Електронні копії зберігаються в єдиному екземплярі на локальному мережевому накопичувачі, що не захищає їх від навмисного знищення шифрувальниками, логічних пошкоджень чи фізичного руйнування. Водночас поточні заходи захисту периметра та плани інтеграції з платформою MISP залишатимуться формальними без впровадження систем активного реагування (SIEM/NGFW) та проактивного моніторингу.

Отже, сучасний стан системи цифрового архівування установи характеризується високим рівнем загрози для електронних ресурсів, що вимагає негайного впровадження надійних політик резервного копіювання, відмови від деструктивних форматів стиснення та реструктуризації мережевої безпеки.

РОЗДІЛ 3. АРХІТЕКТУРННІ ЗМІНИ ТА ПРОЄКТУВАННЯ СИСТЕМИ ДОВГОСТРОКОВОГО ЗБЕРЕЖЕННЯ ЦИФРОВИХ ОБ'ЄКТІВ У ДЕРЖАВНОМУ АРХІВІ РІВНЕНСЬКОЇ ОБЛАСТІ

3.1. Інфраструктурна модернізація та стратегія оркестрації платформи Archivematica

Усунення виявлених недоліків IT-інфраструктури архіву потребує масштабного оновлення дискової та мережевої архітектури. Насамперед інституції необхідно відмовитися від використання апаратних масивів RAID 5, оскільки вони створюють перманентний ризик втрати даних внаслідок невідновлюваних помилок читання (URE).

Технологічним вирішенням цієї проблеми є розгортання кластерної інфраструктури на базі гіпервізора першого типу Proxmox VE із використанням програмно-визначеної файлової системи ZFS (Zettabyte File System). Архітектура дискової підсистеми змінюється шляхом створення пулів ZFS із топологією RAID-Z2 (подвійна парність), що дозволяє масиву гарантовано пережити одночасну відмову двох жорстких дисків без ризику фатального краху внаслідок URE. Вбудовані механізми ZFS, такі як постійна криптографічна перевірка 256-бітних контрольних сум (наприклад, SHA-256) під час кожного звернення до файлу та копіювання під час запису, забезпечують автоматичне виявлення та прозоре самовідновлення пошкоджених блоків, надійно захищаючи архівні фонди від гниття бітів [60], [61].

Перехід на файлову систему ZFS сприяє підвищенню загальної енергоефективності серверного обладнання архіву. Апаратні алгоритми потокового стиснення (наприклад, LZ4) дозволяють відчутно зменшити обсяг файлів, що економить дисковий простір та скорочує потребу в закупівлі

нових накопичувачів. Такий підхід допомагає установі відповідати новим екологічним критеріям (environmental sustainability), передбаченим стандартом NDSA Levels of Digital Preservation 2.1 [28], [52].

Другим стратегічним напрямком інфраструктурної модернізації є ліквідація пласкої топології локальної мережі. Для забезпечення принципу ешелонованої оборони впроваджується концепція «Інфраструктура як код» (Infrastructure as Code - IaC) за допомогою системи конфігураційного управління Ansible. Використання спеціалізованих декларативних модулів (наприклад, ios_vlans) дозволяє автоматизувати процес створення віртуальних локальних мереж (VLAN) на всьому парку комутаторів установи, ізолюючи сервери зберігання від робочих станцій читального залу. Ідемпотентність сценаріїв Ansible гарантує безперебійність роботи мережі під час розгортання політик безпеки, що надійно блокує можливості для розповсюдження програм-вимагачів. Додатковим рівнем проактивного захисту виступає інтеграція платформи MISP через REST API з корпоративним міжмережевим екраном (NGFW), що забезпечує автоматичне блокування шкідливого трафіку на основі індикаторів компрометації (IoC) у режимі реального часу [20].

Основою оновленої архітектури збереження має стати впровадження відкритої платформи Archivematica, яка забезпечує повну алгоритмічну відповідність новітній третій редакції моделі OAIS (формалізованій як міжнародний стандарт ISO 14721:2025) [37].

Всупереч поширеним практикам використання контейнеризації у розробці програмного забезпечення, розгортання Archivematica у виробничому середовищі архіву (production environment) не здійснюватиметься за допомогою Docker-контейнерів.

Згідно з офіційною документацією компанії-розробника Artefactual Systems, інсталяція ядра системи через Docker категорично не підтримується

для production-навантажень через ризики втрати стійкості та продуктивності. Замість цього, архітектура будуватиметься шляхом розгортання пакетів на базі операційних систем сімейства Linux (Ubuntu 22.04 або Rocky Linux 9) з використанням офіційних автоматизованих сценаріїв Ansible на ізольованих віртуальних машинах під управлінням гіпервізора Proxmox [21].

Критичним викликом для нової архітектури є ресурсне голодування, спричинене переходом від збереження файлів у форматі JPEG (із втратами) до генерування майстер-копій (AIP) у нестисненому форматі TIFF. Процес масової міграції форматів вимагає надзвичайно високих обчислювальних потужностей. Згідно з офіційними рекомендаціями, для забезпечення життєздатності системи під час обробки багатогігабайтних колекцій необхідно застосувати стратегію горизонтального масштабування (Scaling out) [21].

Архітектурний патерн масштабування передбачає відокремлення головного сервера управління завданнями (MCPServer) від обчислювальних вузлів (MCPClient). Для прискорення процесів екстракції метаданих, генерації контрольних сум та транскодування зображень, у кластері Proxmox розгортається кілька віртуальних машин MCPClient, які паралельно обробляють черги завдань, розвантажуючи ядро системи. Крім того, під час надходження надзвичайно великих трансферів, конфігурація системи дозволяє працювати у режимі без повнотекстової індексації (indexless mode), відключаючи ресурсоємний мікросервіс Elasticsearch для запобігання тайм-аутам [21].

Цей автоматизований конвеєр гарантує сувору екстракцію технічних метаданих та генерацію криптографічно захищеного словника збереження PREMIS 3.0, що формує безперервний ланцюжок довізного контролю (chain of custody) для кожного цифрового об'єкта [32].

3.2. Багаторівневе резервне копіювання, імутабельність та інтеграція з вимогами eIDAS 2.0

Формування надійного цифрового сховища завершується побудовою ешелонованої системи аварійного відновлення, яка повністю ліквідує залежність архіву від єдиного локального накопичувача. Архітектура збереження будується на базовому галузевому правилі «3-2-1».

Для протидії сучасним загрозам, зокрема цілеспрямованим атакам вірусів-вимагачів на резервні копії, впроваджується концепція кіберсховищ (Cyber Vaulting). Інфраструктура передбачає створення локальних серверів резервного копіювання з «повітряним зазором» (air gap), які фізично відключаються від мережі після завершення інкрементних сесій бекапу. На рівні файлових систем ZFS застосовуються жорсткі політики імутабельності (WORM - Write Once, Read Many), які на апаратно-програмному рівні блокують будь-які спроби модифікації або видалення резервних копій навіть у разі повної компрометації облікових записів адміністратора. Забезпечення географічної надлишковості досягається шляхом асинхронного вивантаження зашифрованих копій пакетів AIP до спеціалізованих хмарних сховищ класу Amazon S3 Glacier, які підтримують функцію Object Lock (хмарний WORM) та інтегруються з архітектурою OCFL [32].

Оновлення інфраструктури дозволить архіву підготуватися до виконання вимог європейського Регламенту 2024/1183 (eIDAS 2.0). Відповідно до статті 45j цього документа, система зможе забезпечувати послугу «кваліфікованого електронного архівування». Це означає, що завантажені до бази документи офіційно зберігатимуть свою юридичну силу та цілісність, відповідаючи стандартам довірчих послуг Європейського Союзу. Таким чином, інфраструктурна модернізація перетворює Державний

архів Рівненської області із локального сховища файлів на стратегічного суб'єкта формування єдиного цифрового довірчого середовища [29].

3.3. Практичні рекомендації щодо впровадження системи збереження цифрових об'єктів у Державному архіві Рівненської області

Впровадження спроєктованої системи збереження цифрової інформації в вимагає від Державного архіву Рівненської області чіткої стратегії, оскільки одномоментний перехід на новітню архітектуру є неможливим через бюджетні обмеження та особливості функціонування установи в умовах воєнного стану.

Для забезпечення безперервності роботи архіву та мінімізації ризиків втрати даних під час міграції, розроблено покроковий план модернізації, розрахований на 2 роки. Він поділений на п'ять функціональних етапів, кожен з яких супроводжується конкретними рекомендаціями.

1. Організаційно-нормативна підготовка та аудит процесів оцифрування

Будь-яка технологічна модернізація повинна починатися зі зміни внутрішніх політик управління.

- **Ревізія форматів оцифрування:** Керівництву необхідно видати внутрішній наказ щодо негайної заборони використання формату JPEG для створення майстер-копій. Усі нові процеси масового сканування повинні бути жорстко переведені на використання нестисненого формату TIFF або стандартизованого JPEG 2000. Це зупинить створення зображень, які не підлягають довгостроковому архівуванню.
- **Створення робочої групи з ІТ-безпеки:** Необхідно формалізувати процеси управління змінами. До складу групи мають увійти керівництво архіву, системний адміністратор та головний зберігач фондів.

Першочерговим завданням групи є проведення самооцінки зрілості цифрового сховища за моделлю DPC RAM, щоб візуалізувати розриви у компетенціях.

- **Розробка регламентів безпеки (СУІБ):** Відповідно до вимог ISO 27001, розробити Політику контролю доступу. Ця політика повинна прямо заборонити зберігання службових паролів у відкритому вигляді та використання єдиного облікового запису для різних співробітників у читальних залах і відділі оцифрування.

2. Базова інфраструктурна модернізація та мережева сегментація

Цей етап присвячений ліквідації найбільш критичних вразливостей (пласкої мережі та децентралізованого управління).

- **Мікросегментація мережі:** Системному адміністратору необхідно розгорнути систему конфігураційного управління Ansible. За допомогою декларативних модулів створити щонайменше три ізольовані віртуальні локальні мережі (VLAN):

VLAN 10 (Службова) — для робочих станцій співробітників відділу оцифрування та канцелярії;

VLAN 20 (Публічна) — виключно для комп'ютерів у читальному залі (з ізоляцією портів і забороною доступу до внутрішніх ресурсів архіву);

VLAN 30 (Серверна) — для NAS-сховищ та майбутнього кластера Proxmox. Маршрутизація між мережами має бути жорстко обмежена правилами міжмережевого екрана за принципом заборони за замовчуванням (Default Deny).

- **Впровадження служби каталогів:** Для усунення децентралізованого управління доступом рекомендується розгорнути відкриту систему ідентифікації (наприклад, FreeIPA або Samba Active Directory), інтегрувавши всі 40 робочих станцій у єдиний домен. Це

дозволить примусово включити політику складності паролів та автоматичне блокування екранів при бездіяльності.

3. Реорганізація дискової підсистеми та впровадження правила «3-2-1»

Найбільш ресурсомісткий етап, спрямований на захист даних від втрати та гниття бітів.

- **Міграція на ZFS:** Застарілу архітектуру RAID 5 на NAS Synology необхідно поетапно вивести з експлуатації. Рекомендується перепрофілювати наявні або закупити нові сервери, встановивши на них гіпервізор Proxmox VE. Жорсткі диски великого об'єму (від 10 ТБ) слід об'єднати в пул ZFS із топологією RAID-Z2.
- **Запуск локального Air-gap бекапу:** Для реалізації правила «3-2-1» необхідно облаштувати фізично відокремлений сервер резервного копіювання. Він повинен бути налаштований за принципом «кіберсховища»: сервер підключається до мережі через скрипт лише в нічний час (наприклад, з 02:00 до 04:00) для отримання інкрементних копій (ZFS Send/Receive), після чого порт на комутаторі автоматично вимикається (Air-gap).
- **Хмарна імутабельність:** Налаштувати асинхронне вивантаження зашифрованих контейнерів із найціннішими документами у хмарні сховища Amazon S3 Glacier. Обов'язково активувати функцію Object Lock (режим Compliance) терміном мінімум на 5 років, що гарантовано захистить копії від програм-вимагачів.

4. Розгортання та налаштування платформи Archivematica (Місяці 11-16) Після створення надійної апаратної бази установа переходить до впровадження логічної моделі OAIS.

- **Кластерна інсталяція:** Розгорнути Archivematica на віртуальних машинах під управлінням Ubuntu 22.04. Використати стратегію

масштабування: встановити один MCPServer та кілька MCPClient для паралельної обробки важких файлів TIFF.

- **Налаштування конвеєра (Ingest):** Налаштувати автоматичну генерацію AIP-пакетів. Заборонити ручну зміну метаданих — система повинна самостійно генерувати словники PREMIS 3.0 та METS-контейнери для створення довізного ланцюжка (chain of custody).
- **Інтеграція з національними порталами:** Оскільки архів має жорсткий ліміт на 500 ГБ для власного вебсайту, необхідно повністю відмовитися від надання послуг через Google Drive. Згенеровані у платформі Archivematica DIP-пакети (копії для доступу у форматі PDF) слід налаштувати на автоматичну передачу до міжархівного пошукового порталу «Архіум».

5. Завершення побудови СУІБ, Threat Intelligence та сертифікація

- **Активна кібербезпека (MISP):** Завершити інтеграцію платформи MISP. Замість пасивного читання індикаторів компрометації (IoC), налаштувати REST API скрипти для автоматичної передачі шкідливих IP-адрес на корпоративний файрвол (NGFW) для миттєвого блокування трафіку (чорні списки).
- **Документування та eIDAS 2.0:** Провести внутрішній аудит усіх журналів системи Archivematica, ZFS та бекапів на предмет відповідності стандарту ISO 16363. Це сформує необхідну доказову базу для Державної архівної служби та Міністерства юстиції щодо готовності архіву до надання послуги «Кваліфікованого електронного архівування» відповідно до норм ЄС.
- **Залучення грантового фінансування та навчання:** Оскільки впровадження ZFS, Linux та Archivematica вимагає високої кваліфікації, керівництву архіву доцільно звернутися до міжнародних програм, які спеціалізуються на захисті культурної спадщини. Отримані кошти слід

спрямувати на закупівлю серверного обладнання та оплату вузькоспеціалізованих курсів підвищення кваліфікації для працівників ІТ-сектору.

ВИСНОВКИ ДО РОЗДІЛУ 3

Запропонований архітектурний реінжиніринг вимагає зміни підходів до побудови мережевої та дискової архітектури для ліквідації критичних вразливостей IT-інфраструктури Державного архіву Рівненської області. Модернізація закладає необхідний технологічний базис для виконання вимог новітнього європейського законодавства.

Зокрема, інфраструктурна модернізація вирішує проблему загрози втрати даних шляхом міграції з апаратних масивів RAID 5 на кластерну інфраструктуру (гіпервізор Proxmox VE) із програмно-визначеною файловою системою ZFS та топологією RAID-Z2. Вбудовані механізми ZFS гарантують автоматичне виявлення та прозоре лікування пошкоджених блоків, надійно захищаючи дані від гниття бітів , тоді як застосування алгоритмів потокової компресії зменшує фізичний розмір інформації та забезпечує відповідність стандартам екологічної стійкості NDSA. Водночас ліквідується пласка топологія локальної мережі за рахунок впровадження концепції «Інфраструктура як код» (Ansible) для автоматизованого створення VLAN. Це, разом з інтеграцією платформи MISP із корпоративним міжмережевим екраном (NGFW), блокує можливості для розповсюдження програм-вимагачів.

Концептуальним ядром оновленої системи стає платформа оркестрації Archivematica, яка забезпечує повну алгоритмічну відповідність моделі OAIS (стандарт ISO 14721:2025). Для забезпечення стабільності та продуктивності виробничого середовища система розгортається на ізольованих віртуальних машинах Linux без використання Docker-контейнерів. Аби подолати ресурсне голодування під час створення майстер-копій у нестисненому форматі TIFF, застосовується стратегія горизонтального масштабування. Відокремлення головного сервера управління (MCPServer) від обчислювальних вузлів

(MCPClient) дозволяє паралельно обробляти завдання та генерувати криптографічно захищений словник збереження PREMIS 3.0, формуючи безперервний ланцюжок довізного контролю.

Формування надійного сховища завершується побудовою багаторівневої системи аварійного відновлення за правилом «3-2-1», що повністю ліквідує залежність архіву від єдиного локального накопичувача. Захист від цілеспрямованих атак забезпечується концепцією кіберсховищ із «повітряним зазором» та жорсткими політиками імутабельності (WORM) на рівні ZFS, які блокують модифікацію резервних копій. Для географічної надлишковості застосовується асинхронне вивантаження зашифрованих копій до спеціалізованих хмарних сховищ (Amazon S3 Glacier) із функцією Object Lock. Ця захищена модель дозволяє виконати вимоги Регламенту (ЄС) 2024/1183 (eIDAS 2.0) щодо запровадження «Кваліфікованого електронного архівування», що наділяє збережені документи безперечною доказовою силою на всьому європейському просторі.

Отже, застосування такої моделі перетворює Державний архів Рівненської області із локального сховища файлів на стратегічного суб'єкта формування єдиного цифрового довірчого середовища.

ВИСНОВКИ

У роботі досліджено проблематику довгострокового збереження цифрових документів та запропоновано практичні шляхи модернізації ІТ-інфраструктури на базі Державного архіву Рівненської області. Цифровізація суспільства, перехід до електронного урядування та серйозні загрози, пов'язані з веденням бойових дій в умовах воєнного стану в Україні, назавжди змінили вимоги до функціонування інституцій пам’яті. На основі всебічного аналізу еволюції архівних підходів, технічного аудиту поточної інфраструктури установи та впровадження новітніх міжнародних стандартів, сформульовано такі стратегічні, концептуальні та інженерно-практичні висновки:

Доведено, що розвиток технологій від аналогових до цифрових носіїв інформації супроводжується глибокою, прихованою вразливістю світової документальної спадщини. На відміну від паперу чи пергаменту, цифрові об’єкти - це не статичні матеріальні сутності, а надзвичайно складні логічні конструкції, що вимагають безперервної багатошарової програмної та апаратної інтерпретації для свого відтворення.

Аналіз міжнародного досвіду підтвердив, що ризик втрати електронних документів через застарівання форматів та деградацію фізичних носіїв є об'єктивною проблемою. Для забезпечення цілісності цифрових даних архівні установи змушені переходити від пасивного зберігання файлів на жорстких дисках до проактивного управління їхнім життєвим циклом. Статистика, що охоплює вибірку з понад 7,4 мільйона цифрових ідентифікаторів об'єктів (DOI), беззаперечно доводить великий масштаб цієї проблеми: понад 27% сучасного світового наукового контенту перебуває під критичною загрозою повного зникнення. Це спростовує поширений інституційний міф про те, що

формальна публікація файлу в мережі Інтернет чи його просте резервне копіювання дорівнює надійному архівному збереженню. Економічні моделі розрахунку життєвого циклу інформації (такі як європейські проєкти LIFE та KRDS) остаточно доводять фінансову нежиттєздатність моделі «збережи і забудь». Забезпечення довгострокового збереження вимагає від держави постійних інвестицій в організаційну інфраструктуру, стандартизацію багатих метаданих та процеси логічної міграції або розгортання середовищ емуляції.

Встановлено, що безальтернативним каркасом для побудови надійних цифрових сховищ є впровадження міжнародного архітектурного стандарту Відкритої архівної інформаційної системи - OAIS (у його найновітнішій редакції ISO 14721:2025). Імплементація цієї моделі докорінно змінює технологічний процес діловодства: інформація більше ніколи не зберігається як набір «сирих», розрізнених файлів. Замість цього вона жорстко інкапсулюється у стандартизовані Інформаційні пакети подання (SIP), криптографічно захищені Архівні інформаційні пакети (AIP - еталонні майстер-копії) та зручні для користувачів Інформаційні пакети розповсюдження (DIP). Для збереження доказової сили електронних документів необхідно впроваджувати спеціалізовані стандарти метаданих, такі як PREMIS 3.0 та RiC-O. Вони забезпечують безперервне документування історії змін файлів під час їх міграції або відтворення.

Тільки створення суворого, алгоритмічно підтвердженого ланцюжка довізного контролю (chain of custody) через детальне машинне документування об'єктів, відповідальних агентів, інтелектуальних прав і кожної події трансформації формату здатне нівелювати ризики компрометації доказової сили документа під час його неминучої майбутньої програмної міграції.

Проведений у роботі аудит організації, процесів оцифрування та загальної IT-інфраструктури досліджуваної регіональної установи виявив значні розриви між її поточним станом та жорсткими вимогами міжнародних критеріїв надійності (таких як стандарт аудиту ISO 16363 та модель DPC RAM). Попри зафіксовані рекордні темпи масового сканування історичних документів (зокрема генеалогічних метричних книг), виявлено такі загрози:

1. **Логічна деградація та спотворення фондів:** Використання формату JPEG (алгоритму стиснення із втратами) для генерації майстер-копій (AIP) через брак дискового простору є грубим порушенням принципів архівного збереження. Це неминуче призводить до кумулятивної генераційної деградації піксельної інформації під час багаторазових переглядів та майбутніх міграцій. Визнаним стандартом збереження візуальних матеріалів повинні стати виключно нестиснені формати (TIFF або стандартизований JPEG 2000 Lossless).

2. **Стан апаратної архітектури зберігання:** Використання мережевого сховища (NAS) на базі застарілої технології RAID 5 з жорсткими дисками великої ємності формує ризик повної втрати всього логічного тому через математично гарантовані невідновлювані помилки читання (URE) під час процесу реконструкції масиву. Ситуація ускладнюється повною відсутністю системи резервного копіювання, що прямо ігнорує правило «3-2-1». Ця недбалість залишає петабайти унікальних оцифрованих історичних документів беззахисними перед апаратними збоями, логічними помилками або цілеспрямованими деструктивними діями програм-вимагачів (ransomware).

3. **Кібернетична незахищеність та мережева вразливість:** Наявність в установі єдиної пласкої топології локальної мережі (Flat Network без мікросегментації та VLAN) і повна відсутність централізованого

управління ідентифікацією користувачів (такого як Active Directory) створюють ідеальні тепличні умови для безперешкодного латерального переміщення шкідливого програмного забезпечення від звичайних комп'ютерів у відкритому читальному залі безпосередньо до критичних серверів збереження бази даних.

Для оперативної ліквідації виявлених вразливостей у роботі розроблено та обґрунтовано детальний інженерний проєкт модернізації системи цифрового архівування. Запропонована архітектура глибоко спирається на підхід «Безпека за замовчуванням» (Security by Design) і передбачає такі кроки:

1. **Міграція на програмно-визначені сховища даних (ZFS):** Категорична відмова від використання апаратного RAID 5 на користь розгортання надпотужного кластера на базі гіпервізора першого типу Proxmox VE із використанням передової файлової системи ZFS (топологія RAID-Z2). Це гарантує абсолютний захист від помилок URE при виході з ладу до двох жорстких дисків одночасно. Вбудовані механізми копіювання під час запису (Copy-on-Write) і постійна валідація 256-бітних криптографічних контрольних сум забезпечують прозоре, фонове і автоматичне «лікування» гниття бітів, гарантуючи фізичну імутабельність потоків даних. Крім того, застосування алгоритмів потокової компресії (LZ4) відповідає найновішим екологічним критеріям стійкості центрів обробки даних, затвердженим матрицею NDSA версії 2.1.

2. **Мережева мікросегментація та проактивний моніторинг:** Впровадження сучасної концепції «Інфраструктура як код» (IaC) за допомогою систем управління конфігураціями (Ansible) для швидкого та автоматизованого налаштування ізольованих VLAN. Це, разом з глибокою програмною інтеграцією національної платформи Threat Intelligence (MISP) із

системами активного реагування та міжмережевими екранами (NGFW), надійно блокує потенційні вектори атак хакерів і формує систему ешелонованої оборони, що повністю відповідає міжнародним стандартам серії ISO/IEC 27000 та жорстким настановам кібербезпеки NIST SP 800-209.

3. **Автоматизація оркестрації життєвого циклу (платформа Archivematica):** Запропоновано розгортання потужної платформи Archivematica на базі ізольованих віртуальних машин Linux (з категоричною відмовою від використання нестабільних для виробничого середовища Docker-контейнерів, згідно з офіційними рекомендаціями). Застосування стратегії горизонтального масштабування (з чітким відокремленням головного вузла MCPServer від пулу обчислювальних вузлів MCPClient) дозволить архіву успішно подолати ресурсне голодування серверів під час інтенсивного транскодування петабайтних масивів відсканованих зображень у формат TIFF і генерування вичерпних криптографічних словників PREMIS.

Надана архітектурна модернізація має не лише суто технічне, але й надзвичайно глибоке правове та політичне значення для держави. Забезпечення імутабельності на рівні файлової системи (WORM - Write Once, Read Many) та створення географічно розподілених «кіберсховищ» (Cyber Vaulting) з фізичними «повітряними зазорами» створює потужний технологічний фундамент для імплементації в щоденну діяльність архіву жорстких вимог новітнього європейського Регламенту (ЄС) 2024/1183 (eIDAS 2.0). Перехід українських інституцій до надання офіційної послуги «Кваліфікованого електронного архівування автоматично наділятиме збережені в базах електронні документи презумпцією бездоганної цілісності та юридичною доказовою силою, що беззаперечно визнаватиметься на всій території Європейського Союзу.

Усунення виявлених недоліків у топології мережі та системах зберігання Державного архіву області дозволить суттєво підвищити надійність його фондів. Реалізація запропонованих рішень (міграція на ZFS, мікросегментація мережі та впровадження платформи Archivematica) забезпечить захист електронних ресурсів від апаратних збоїв та сучасних кіберзагроз. Подальша оптимізація ІТ-процесів та інтеграція регіонального архіву до національного пошукового порталу «Архіум» сприятимуть створенню безпечної та відкритої системи доступу громадян до історичної документації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державна архівна служба України. Міжархівний пошуковий портал. URL: https://searcharchives.net.ua/ (дата звернення: 12.06.2026).

2. Державна архівна служба України. Офіційний вебпортал. URL: https://archives.gov.ua/ua/ (дата звернення: 12.06.2026).

3. Державна архівна служба України. Офіційні звіти щодо оцифрування та збереження фондів в умовах воєнного стану. 2024.

4. Державна податкова служба України. Роз'яснення ДПС України щодо ЗУ. URL: https://sumy.tax.gov.ua/media-ark/news-ark/print-842770.html (дата звернення: 12.06.2026).

5. Державний архів Рівненської області. Офіційний вебсайт. URL: https://rv.archives.gov.ua/ (дата звернення: 12.06.2026).

6. Державний архів Рівненської області. Оцифровані справи. URL: https://rv.archives.gov.ua/ocifrovani-sprav?period=5 (дата звернення: 12.06.2026).

7. ДНАОП. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. URL: https://dnaop.com/html/62498/doc-%D0%94%D0%A1%D0%A2%D0%A3_ISO_IEC_27001_2015 (дата звернення: 12.06.2026).

8. ДСТУ 2732:2023. Діловодство й архівна справа. Терміни та визначення понять. Київ : ДП «УкрНДНЦ», 2023.

9. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови щодо ідентифікації, збирання, одержання та збереження цифрових доказів.

10. Законодавство України, Документ № n0012323-12. URL:

https://zakon.rada.gov.ua/laws/show/n0012323-12 (дата звернення: 12.06.2026).

11. Зберігання електронних документів: електронні архіви України. Вчасно. 2023. URL: https://vchasno.ua/en/elektronni-arhivy-ukrainy/ (дата звернення: 12.06.2026).

12. Про авторське право і суміжні права : Закон України. URL: https://zakon.rada.gov.ua/laws/show/2811-20 (дата звернення: 12.06.2026).

13. Про електронні документи та електронний документообіг: Закон України № 851-IV від 22.05.2003 р.

14. Про захист персональних даних : Закон України. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 12.06.2026).

15. Про Національний архівний фонд та архівні установи: Закон України № 3814-XII від 24.12.1993 р.

16. Рівненська обласна державна адміністрація. Положення про Державний архів Рівненської області. URL: https://www.rv.gov.ua/polozhennya-pro-derzhavnij-arhiv-rivnenskoyi-oblasti (дата звернення: 12.06.2026).

17. Цецик Я., Шамало І.Роль цифрових технологій у зберіганні архівної інформації. *Вісник науки та освіти*. 2026. № 4(46). С. 5672–5680.

18. Україна на передовій цифровізації: Естонія ознайомилася з українським досвідом оцифрування архівних документів. Урядовий портал. 2024. URL: https://www.kmu.gov.ua/en/news/ukraina-na-peredovii-tsyfrovizatsii-estoniia-oznaiomylasia-z-ukrainskym-dosvidom-otsyfruvannia-arkhivnykh-dokumentiv (дата звернення: 12.06.2026).

19. Центральний державний електронний архів України (ЦДЕАУ). Електронний архів (е-Архів).

20. Ansible. cisco.ios.ios_vlans module. Ansible Documentation. URL:

https://docs.ansible.com/projects/ansible/latest/collections/cisco/ios/ios_vlans_module.html (дата звернення: 12.06.2026).

21. Archivematica. Archivematica Documentation. URL: https://www.archivematica.org/en/docs/ (дата звернення: 12.06.2026).

22. Backblaze. The 3-2-1 Backup Strategy. Backblaze Blog. URL: https://www.backblaze.com/blog/the-3-2-1-backup-strategy/ (дата звернення: 12.06.2026).

23. CCSDS 650.0-M-2. Reference Model for an Open Archival Information System (OAIS). Magenta Book, 2012.

24. Chandramouli R., Pinhas D. NIST SP 800-209: Security Guidelines for Storage Infrastructure. National Institute of Standards and Technology, 2020.

25. Cisco. Cisco Umbrella. URL: https://umbrella.cisco.com/ (дата звернення: 12.06.2026).

26. CNI. JISC Keeping Research Data Safe 2 Final Report. URL: https://www.cni.org/news/jisc-keeping-research-data-safe-2-final-report (дата звернення: 12.06.2026).

27. Digital Preservation Coalition (DPC). Digital Preservation Coalition Rapid Assessment Model (DPC RAM), Version 3. 2024. URL: http://doi.org/10.7207/dpcram24-03 (дата звернення: 12.06.2026).

28. Digital Preservation Coalition (DPC). NDSA releases Levels of Digital Preservation version 2.1. URL: https://www.dpconline.org/news/ndsa-releases-levels-of-digital-preservation-version-2-1 (дата звернення: 12.06.2026).

29. Entrust. What is eIDAS? URL: https://www.entrust.com/resources/learn/eidas (дата звернення: 12.06.2026).

30. European Union. eIDAS 2.0. European Digital Identity Regulation. 2024. URL:

https://www.european-digital-identity-regulation.com/Article_45_(Regulation_EU_2024_1183).html (дата звернення: 12.06.2026).

31. Eve M. P. et al. Digital Scholarly Journals Are Poorly Preserved: A Study of 7 Million DOIs. Journal of Librarianship and Scholarly Communication. 2024.

32. Fedora Repository. Fedora and the NDSA Levels of Digital Preservation. URL: https://fedorarepository.org/fedora-ndsa-levels-digital-preservation/ (дата звернення: 12.06.2026).

33. Granger S. Emulation as a Digital Preservation Strategy. D-Lib Magazine. 2000. Vol. 6, № 10.

34. Hodge G. Best Practices for Digital Archiving. D-Lib Magazine. 2000. Vol. 6, № 1.

35. Holtstrom M. RAID 5 URE Failures. Blog. URL: https://holtstrom.com/michael/blog/post/588/RAID-5-URE-Failures.html (дата звернення: 12.06.2026).

36. International Council on Archives. Records in Contexts Ontology (RiC-O) Version 1.1. URL: https://www.ica.org/standards/RiC/RiC-O_1-1.html (дата звернення: 12.06.2026).

37. ISO 14721:2012. Space Data and Information Transfer Systems – Open Archival Information System (OAIS) – Reference Model. 2012.

38. ISO 16363:2012. Space Data and Information Transfer Systems – Audit and Certification of Trustworthy Digital Repositories. 2012.

39. ISO 31000:2018. Risk Management – Guidelines. 2018.

40. ISO/IEC 27000:2018. Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. 2018.

41. Joan Mitchell Foundation. CALL Digital Media Resources. URL:

https://www.joanmitchellfoundation.org/uploads/pdf/CALL-Digital_Media_Resources.pdf (дата звернення: 12.06.2026).

42. Kuny T. The Digital Dark Ages? Challenges in the Preservation of Electronic Information. International Preservation News. 1998. № 17.

43. Library of Congress. METS Version 2. URL: https://www.loc.gov/standards/mets/mets2.html

44. Marchenko V. Information Security and Long-Term Digital Preservation in Public Governance: Regulatory Alignment, Archival Integrity, and Technology Choices. Public Administration and Law Review. 2025. Vol. 4, № 24. P. 68–77.

45. Metron Labs. Bringing MISP into Google SecOps: A Practical Integration Architecture. URL: https://hub.metronlabs.com/bringing-misp-into-google-secops-a-practical-integration-architecture/ (дата звернення: 12.06.2026).

46. Microsoft. Microsoft Cloud Security Benchmark: Identity Management. Microsoft Learn. URL: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-identity-management (дата звернення: 12.06.2026).

47. miniOrange. How to Detect and Prevent Lateral Movement. miniOrange Blog. URL: https://www.miniorange.com/blog/detect-prevent-lateral-movement/ (дата звернення: 12.06.2026).

48. MISP Project. MISP Tools. URL: https://www.misp-project.org/tools/ (дата звернення: 12.06.2026).

49. Mojjada H. Protocol for Metadata Harvesting: The Role of OAI-PMH in Digital Resource Integration. International Journal of Research and Innovation in Applied Science. 2025. Vol. 10, № 7. P. 724–736.

50. National Archives and Records Administration (NARA). Digital Preservation Strategy 2022–2026. 2022.

51. NDSA. Announcing Version 2.1 of the NDSA Levels of Digital Preservation. Mar. 2026. URL: https://www.ndsa.org/2026/03/23/announcing-version-2_1-of-the-ndsa-levels-of-digital-preservation.html (дата звернення: 12.06.2026).

52. NDSA. Preservation Storage Topic: JPEG2000. DLF Wiki. URL: https://wiki.diglib.org/NDSA:Preservation_Storage_Topic_JPEG2000 (дата звернення: 12.06.2026).

53. Need To Know IT. NAS File Systems Explained: EXT4 vs BTRFS vs ZFS. URL: https://needtoknowit.com.au/blog/nas-file-systems-explained-ext4-vs-btrfs-vs-zfs/ (дата звернення: 12.06.2026).

54. Novytskyi O. Metadata Harvesting for Digital Library Integration in Ukraine: A Comparative Study of the OAI-PMH Protocol and VuFind's Efficacy. Digital Library Perspectives. 2025. Vol. 41, № 1. P. 74–90.

55. PDF Association. ISO 19005 (PDF/A). URL: https://pdfa.org/resource/iso-19005-pdfa/ (дата звернення: 12.06.2026).

56. Pew Research Center. When Online Content Disappears. May 2024. URL: https://www.pewresearch.org/data-labs/2024/05/17/when-online-content-disappears/ (дата звернення: 12.06.2026).

57. PREMIS Editorial Committee. PREMIS Data Dictionary for Preservation Metadata, Version 3.0. Library of Congress, 2015.

58. Preservica. What You Need to Know About the Most Recent OAIS Revision. Preservica Blog. URL: https://preservica.com/resources/blogs-and-news/what-you-need-to-know-about-th

e-most-recent-oais-revision (дата звернення: 12.06.2026).

59. Proxmox. Proxmox Server Solutions. URL: https://www.proxmox.com/en/ (дата звернення: 12.06.2026).

60. RAIDZ Calculator. RAID-Z Types Reference. URL: https://www.raidz-calculator.com/raidz-types-reference.aspx (дата звернення: 12.06.2026).

61. Reddit. BTRFS vs EXT4: Long term stability after 3 years. r/synology. URL: https://www.reddit.com/r/synology/comments/1t4409y/btrfs_vs_ext4_long_term_stability_after_3_years/ (дата звернення: 12.06.2026).

62. Rosenthal D. S. H. et al. Transparent Format Migration of Preserved Web Content. D-Lib Magazine. 2005.

63. Rothenberg J. Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation. Washington, D.C. : Council on Library and Information Resources, 1999.

64. Software Preservation Network. EaaSI Research Alliance. URL: https://www.softwarepreservationnetwork.org/eaasi-research-alliance/ (дата звернення: 12.06.2026).

65. Super User. Are RAID 5 systems suitable for larger disk sizes? URL: https://superuser.com/questions/912673/are-raid-5-systems-suitable-for-larger-disk-sizes (дата звернення: 12.06.2026).

66. Synology Community. RAID and Storage Discussion Thread. URL: https://community.synology.com/enu/forum/17/post/79816 (дата звернення: 12.06.2026).

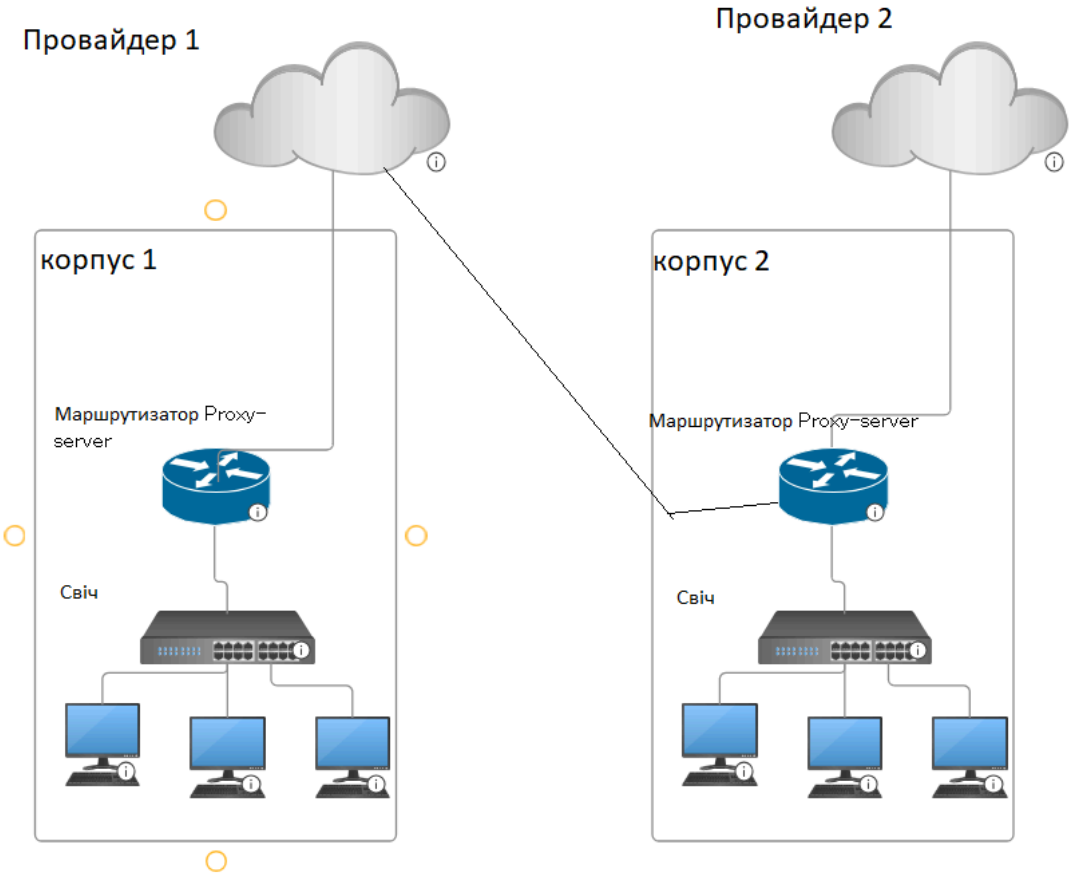
67. Trendyol Tech. MISP Threat Sharing. Medium. URL: https://medium.com/trendyol-tech/misp-threat-sharing-d7f0fd236fb5 (дата звернення: 12.06.2026).

68. Tufin. Navigating the Perils: Flat Network Security Risks. Tufin Blog. URL: https://www.tufin.com/blog/navigating-perils-flat-network-security-risks (дата звернення: 12.06.2026).

69. Wikipedia. RAID. URL: https://en.wikipedia.org/wiki/RAID (дата звернення: 12.06.2026).

70. Zero Networks. Ransomware and Lateral Movement Protection Blueprint. URL: https://zeronetworks.com/resource-center/topics/ransomware-and-lateral-movement-protection-blueprint (дата звернення: 12.06.2026).

Додаток А


Провайдер 1
Провайдер 2
корпус 1
корпус 2
Маршрутизатор Proxy-server
Маршрутизатор Proxy-server
Свіч
Свіч